UNL • FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES

Tesis Doctoral

Doctorado en Derecho

Facultad de Ciencias Jurídicas y Sociales

Universidad Nacional del Litoral

Delitos Informáticos y Cibercrimen:

Un Estudio de Derecho Comparado de Aspectos de Derecho Penal y Procesal Penal con Enfoque en la Elaboración de una Guía de Buenas Prácticas para la solicitud de Medidas o Técnicas Especiales de Investigación para casos de Cibercrimen

Doctorando: Abog. Marcelo Temperini

Director de Tesis: Dr. Federico Fumis

"El pesimista se queja del viento; el optimista espera que cambie y el realista ajusta las velas"

George Ward

Índice de contenido

Índice de contenido 3
Agradecimientos: 12
Introducción: 13
1.1. Delimitación del objeto 15
1.2. Situación problemática 16
1.3. Construcción de Hipótesis y Objetivos 18
1.3.1. Hipótesis a validar 18
1.3.2. Objetivos Específicos 18
1.3.3. Objetivos Generales 19
1.4. Antecedentes personales 20
1.5. Metodología y marco conceptual 25
Capítulo I: La eficacia del Derecho en los delitos Informáticos 26
1.1. Introducción 26
1.2. El Derecho y su función de control social 27
1.3. La Eficacia como valor en el Derecho 28
1.4. Otros conceptos de eficacia 28
1.5. Eficacia: grados y metodología. 30
1.6. La Era de la Sociedad de la Información 32
1.7. Las Tecnologías de la Información y Comunicación y el Derecho 33
1.8. La Eficacia del Derecho en la Sociedad de la Información 36
1.9. El caso de la combinación entre Tecnología y Propiedad Intelectual 37
1.10. El caso de la combinación entre Tecnología y Delincuencia 38
1.11. Los delitos informáticos como un desafío para el Derecho 39
1.12. La eficacia del Derecho en los Delitos Informáticos 40
Capítulo II: Delitos Informáticos y Cibercrimen. 43
2.1. Introducción 43
2.2. Aspectos básicos de la Seguridad de la Información 44
2.3. La tecnología como potenciadora del delito 47
2.4. Delitos Informáticos. Conceptos y alcances 50
2.5. Cibercrimen y ciberdelincuencia 53
2.6. Hackers vs. Crackers 57
2.7. Hacking: categorías y posturas doctrinarias 62
2.8. Expansionismo penal y el riesgo de los delitos de peligro 66
2.9. Delitos informáticos y el bien jurídico protegido 71
2.10. Caracteres de los delitos informáticos 75
2.10.1 Delitos de cuellos blanco 77
2.10.2 Trasnacionales 78
2.10.3 Instantáneos 80
2.10.4 Masivos o Simultáneos 81
2.10.5 Anónimos 82
2.10.6 Pluriofensivos 85
Capítulo III: Estadísticas en ciberdelincuencia 89
3.1. Introducción 89

3.2 Estadísticas corporativas 90
3.3 Estadísticas oficiales a nivel nacional. 91
3.3.1. Estadísticas anuales de la UFEDYCI 91
3.3.2. Muestreos oficiales del Ministerio de Justicia y Derechos Humanos de la Nación Argentina 96
3.4. Los Centros de Respuesta (CSIRT/CERT) 127
3.5. Estadísticas a nivel internacional. 131
3.5.1. El problema de la victimización y la falta de denuncias 132
3.6. La medición del delito 134
3.6.1. Estadísticas delictivas registradas por la policía 135
3.6.2. Estadísticas a la población y a las empresas 140
3.6.3. Iniciativas de denuncia para las víctimas 143
3.6.4. Información sobre seguridad cibernética con base tecnológica 144
3.7 El problema de la cifra negra 146
3.7.1 Estadísticas del Proyecto ODILA 150
Capítulo IV: La tipificación de los delitos informáticos 162
4.1. Introducción 162
4.2. Estudios realizados por la ONUDC 164
4.3. Instrumentos Internacionales sobre Ciberdelito 167
4.3.1. Convenio sobre Ciberdelincuencia Nº 185: (Budapest) 168
4.3.1.1. Primer Protocolo Adicional relativo a la penalización de actos de naturaleza racista y xenófoba cometidos a través de sistemas informáticos (STCE 189) 171
4.3.1.2. Segundo Protocolo adicional al Convenio sobre la Ciberdelincuencia, relativo a la cooperación reforzada y la revelación de pruebas electrónicas. 174
4.3.1.3. Críticas y cuestionamientos al Segundo Protocolo adicional al Convenio sobre la Ciberdelincuencia. 178
4.3.1.4. Aspectos destacados del Convenio 179
4.3.1.5. Argentina y el Convenio sobre la Ciberdelincuencia de Budapest 182
4.3.1.6. Brasil y el Convenio sobre la Ciberdelincuencia de Budapest 184
4.3.1.7. Colombia y el Convenio sobre la Ciberdelincuencia de Budapest 186
4.3.1.8. México y el Convenio sobre la Ciberdelincuencia de Budapest 188
4.3.1.9. España y el Convenio sobre la Ciberdelincuencia de Budapest 191
4.3.2. Proyecto de Convención Internacional Integral sobre la Lucha contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos (ONU) 192
4.3.2.1. Breve cronología del Proyecto 192
4.3.2.2. Observaciones sobre el tratado 200
4.4. Metodología y alcance del estudio 200
4.5. Identificación de marcos normativos aplicables 202
4.5.1. Tipos de marcos jurídicos 202
4.5.2. Relevamiento de normativas aplicables 204
4.6. Relevamiento de delitos informáticos tipificados 206
4.6.1. Cuadro comparativo entre el Convenio de Budapest y el Proyecto de Regulación de la ONU 209
4.6.2. Dificultades metodológicas 214
4.6.3. Delito 1: Acceso ilícito a sistemas o datos informáticos 215
4.6.3.1. Movimiento para la despenalización de la actividad de seguridad informática 219
4.6.4. Delito 2: Interceptación ilícita de datos informáticos 221
4.6.5. Delito 3: Atentado contra la integridad de los datos (cracking o daño informático) 225
4.6.6. Delito 4: Atentados contra la integridad del sistema (Denegación de servicios) 230

4.6.7. Delito 5: Abuso de Dispositivos 235
4.6.8. Delito 6: Falsedad Informática 240
4.6.9. Delito 7: Fraude o Estafa Informática 246
4.6.10. Delito 8: Material de Abuso Sexual Infantil 250
4.6.11. Delito 9: Suplantación de identidad digital 258
4.6.12. Delito 10: Captación ilegítima de datos confidenciales (Phishing) 264
4.6.13. Delito 11: Violación de datos personales 270
4.7. Generación de estadísticas 278
4.8.1. Regulación de delitos por países 279
4.8.2. Nivel de tipificación por delito 281
Capítulo V: La afectación de derechos a través de medidas de injerencia 284
5.1. Introducción 284
5.2. Indicios y Evidencia 285
5.3. Principios probatorios 288
5.3.1. Principio de oportunidad 289
5.3.2. Principio de inmediación 291
5.3.3. Principio de contradicción 292
5.3.4. Principio de libertad probatoria 294
5.3.5. Principio de pertinencia 295
5.3.6. Principio de exclusión 296
5.3.7. Principio de igualdad de oportunidades para la prueba 297
5.4. Evidencia digital en el proceso penal 298
5.4.1. Características de la Evidencia Digital 298
5.4.2. La necesidad de nuevas reglas 301
5.5. Medidas de injerencia (o coerción) y medios de prueba 302
5.5.1. El origen del principio de Nulla coactio sine lege 305
5.5.2. Primer nivel de análisis: existencia y alcance de la medida 306
5.5.3. Segundo nivel de análisis: competencia objetiva 307
5.5.4. Tercer nivel de análisis: competencia subjetiva 308
5.6. La afectación de derechos a través de medidas de investigación penal 311
5.6.1. Las salvaguardas en el Convenio de Budapest 312
5.6.2. Derecho a la privacidad e intimidad 316
5.6.3. Derecho al secreto de las comunicaciones 324
5.6.4. Derecho a la protección de datos personales 328
5.6.5. Derecho al entorno digital 331
5.7. Principios aplicables a medidas de investigación 335
5.7.1. Principio de especialidad 335
5.7.2. Principio de idoneidad 338
5.7.3. Principio de excepcionalidad 340
5.7.4. Principio de necesidad 343
5.7.5. Principio de proporcionalidad 345
5.8. Medidas que no requieren autorización judicial 352
5.8.1. Identificación de dirección IP 352
5.8.2. Identificación de IMEI, IMSI y MAC. 356
5.8.3. Identificación de titulares o terminales o dispositivos de conectividad. 359
5.8.4. Acceso a datos que no forman parte de un proceso de comunicación 361

5.8.5. Interceptación de conversaciones en el espacio público. 363
5.8.6. La regla de los 3 escalones 364
5.8.6.1. El primer escalón: los datos de abonado 366
5.8.6.2. El segundo escalón: los datos de tráfico 372
5.8.6.3. El tercer escalón: los datos de contenido 381
5.9. Un caso de análisis práctico. 383
Capítulo VI: Medidas o técnicas especiales de investigación 387
6.1. Introducción 387
6.2. Estadísticas a nivel internacional 388
6.2.1. Estudio exhaustivo sobre el delito informático (UNODC 2013) 388
6.2.2. Informe sobre Cibercrimen (ONU 2018) 391
6.1. El desafío de la investigación compleja 393
6.2. Medidas de Investigación sugeridas en instrumentos internacionales 400
6.2.1. Conservación rápida de datos informáticos almacenados 417
6.2.2. Conservación y divulgación inmediata de los datos de tráfico 419
6.2.3. Orden de presentación 422
6.2.4. Registro y confiscación de datos informáticos almacenados 423
6.2.5. Obtención en tiempo real de datos informáticos (datos de tráfico / datos de contenido 427
6.3. Otras Medidas o técnicas especiales de investigación 431
6.3.1. OSINT (Open Source Intelligence) 432
6.3.1.1. La legalidad de la técnica desde la óptica de la Protección de Datos Personales 435
6.3.1.2. OSINT y su función en la prevención policial del delito 439
6.3.2. Agente encubierto informático o digital 441
6.3.2.1. La diferencia entre Agente encubierto digital y el Ciberpatrullaje 445
6.3.3. Registro remoto sobre equipos informáticos 447
6.3.3.1. Registro remoto en allanamientos tradicionales 447
6.3.3.2. Registro remoto subrepticio como alternativa al allanamiento 449
6.3.3.3. Los límites como forma de garantía 451
6.3.4. Identificación de dispositivo mediante captación de información de sistema 452
6.3.4.1. La técnica del Browser fingerprinting 453
6.3.4.2. Canvas Fingerprinting 455
6.3.4.3. WEBRTC 456
6.3.4.4. AudioContext 457
6.3.4.5. Una herramienta a tener en cuenta 458
6.3.5. Acceso transfronterizo de datos 459
6.3.5.1. ¿Violación del principio de territorialidad? 460
6.3.5.2. La afectación de la soberanía nacional 462
6.3.5.3. Casos autorizados según el Convenio de Budapest 463
6.3.5.4. La necesidad de regular casos de urgencia 464
6.3.6. Desbloqueo compulsivo de datos informáticos 465
6.3.6.1. Desbloqueo compulsivo en Estados Unidos 466
6.3.6.2. Desbloqueo compulsivo en Argentina 467
6.3.6.3. La existencia o no del contenido comunicacional 469
6.3.7. Hallazgos casuales en la evidencia digital 471
6.3.7.1. La necesidad de repensar la doctrina de la plain view 472
6.3.7.2. Hallazgos casuales según jurisprudencia Argentina 473

6.3.7.3. La diferencia en la afectación de derechos 475
6.3.7.4. La prohibición de utilizar archivos no relacionados con la medida 476
Capítulo VII: Medidas de Investigación previstas en el Derecho Procesal Penal 480
7.1. Introducción: 480
7.1.1. Selección de medidas o técnicas de investigación 481
7.2. Medidas de investigación reguladas en Argentina 483
7.2.1. Código Procesal Penal Federal 483
7.2.1.1. Proyectos que no fueron 484
7.2.1.2. Cuadro de medidas de investigación reguladas 486
7.2.1.3. La regulación del OSINT en contexto de pandemia 489
7.2.1.4. Ciberpatrullaje pero con principios 490
7.2.1.5. La particular situación sobre retención de datos de tráfico en Argentina 492
7.2.2. Ciudad Autónoma de Buenos Aires 495
7.2.2.1. Cuadro de medidas de investigación reguladas 495
7.2.2.2. Prohibición de inspeccionar datos privados 498
7.2.3. Mendoza 500
7.2.3.1. Cuadro de medidas de investigación reguladas 500
7.2.3.2. La figura del agente encubierto informático 505
7.2.3.3. La orden aseguramiento y de presentación de datos 506
7.2.3.4. El registro remoto que no fue 508
7.2.4. Neuquén 509
7.2.4.1. Cuadro de medidas de investigación reguladas 509
7.2.4.2. Conservación, decomiso y registro remoto 512
7.2.4.3. Recolección de comunicaciones en tiempo real 513
7.2.5. Salta 514
7.2.5.1. La generación de una Comisión Reformadora 514
7.2.5.2. Cuadro de medidas de investigación reguladas 515
7.2.5.3. La inclusión del Agente encubierto digital 527
7.2.5.4. Obtención remota de datos de dispositivos informáticos 528
7.2.5.5. La novedad en el Acceso a datos almacenados en extraña jurisdicción 531
7.3. Medidas de investigación reguladas en Brasil 533
7.3.1. El marco civil de internet y su importancia en la investigación 533
7.3.2. La situación de Brasil según la ONU 535
7.3.3. Cuadro de medidas de investigación reguladas 536
7.3.4. La conservación de datos 540
7.3.5. La entrega de datos como reemplazado del mandato de comunicacion 541
7.3.6. La interceptación de las comunicaciones 543
7.3.7. La captura ambiental de señales electromagnéticas, ópticas o acústicas 544
7.4. Medidas de investigación reguladas en Colombia 545
7.4.1. La evolución del marco normativo procesal en Colombia 545
7.4.2. Cuadro de medidas de investigación reguladas 546
7.4.3. Búsqueda selectiva en bases de datos 551
7.4.4. La posibilidad de recuperación de información 554
7.4.5. La interceptación de comunicaciones 555
7.4.6. Operaciones encubiertas en medios de comunicación virtual 556
7.5. Medidas de investigación reguladas en México 557

7.5.1. El Código Nacional de Procedimientos Penales Mexicano 557
7.5.2. Cuadro de medidas de investigación reguladas 558
7.5.3. Conservación de comunicaciones 565
7.5.4. Colaboración con la autoridad y aporte voluntario 567
7.5.5. Intervención de comunicaciones y extracción de información 568
7.5.6. Localización geográfica en tiempo real 569
7.6. Medidas de investigación reguladas en España 571
7.6.1. La Ley de Enjuiciamiento Criminal española 571
7.6.2. Cuadro de medidas de investigación reguladas 572
7.6.3. Orden de conservación de datos 582
7.6.4. Acceso a datos necesarios para la identificación de usuarios y dispositivos 583
7.6.4.1. Identificación por dirección IP 583
7.6.4.2. Identificación de terminales mediante captación de códigos de identificación 584
7.6.4.3. Identificación de titulares, dispositivos o terminales 585
7.6.5. Registro de dispositivos de almacenamiento masivo de información 585
7.6.6. La extensión de registros 587
7.6.7. El acceso a los datos ante casos de urgencia 588
7.6.8. La colaboración de personas que tengan conocimiento del sistema informático 588
7.6.9. Incorporación al proceso de datos electrónicos de tráfico o asociados 590
7.6.10. La posibilidad de registro remoto 590
7.7. Generación de estadísticas 592
7.7.1. Regulación de medidas de investigación por países 597
7.7.2. Nivel de regulación por medida de investigación 600
Capítulo VIII: Conclusiones 602
8.1. Un problema complejo 602
8.2. La tipificación de los delitos informáticos 602
8.2.1. Conclusiones sobre el nivel de normativas vigentes 603
8.2.2. Conclusiones sobre el nivel de tipificación de los delitos informáticos alcanzados 605
8.2.3. Hipótesis 1: ¿Están adecuadamente tipificados los delitos informáticos? 607
8.3. La inexistencia de normas y su relación con la afectación de derechos y garantías 609
8.3.1. ¿Medidas de prueba o medidas de injerencia? 610
8.3.2. ¿Regular o no regular? 611
8.3.2. ¿Afecta la regulación a la potencial afectación de derechos y garantías? 611
8.4. La regulación de las medidas o técnicas especiales de investigación 613
8.4.1. Conclusiones sobre el estudio comparado 613
8.4.2. Conclusiones sobre el nivel de regulación de las medidas o técnicas especiales de investigación por jurisdicción 615
8.4.3. Conclusiones sobre las medidas de investigación reguladas 621
8.4.4. Hipótesis 2: ¿Están adecuadamente reguladas las medidas o técnicas especiales de investigación? 627
8.5. Consideraciones adicionales 629
8.5.1. La asimetría de poder respecto de la investigación 630
8.5.2. Identificar la investigación no convencional o compleja 631
8.5.3. La buena técnica legislativa 632
8.5.4. El cibercrimen con perspectiva: un problema multifactorial 633
8.5.5. El conocimiento como co-construcción 634
8.6. Conclusiones Finales y Generación de Propuesta 635

Capítulo IX: Propuesta Final **638**
1.0. Introducción 638
2.0. Aspectos Generales 639
2.1. Alcance 639
2.2. Misión 639
2.3. Visión 640
2.4. Objetivos generales 641
2.5. Objetivos específicos 641
3.0. Metodología y Desarrollo del Sistema 642
3.1. Ingreso al sistema 642
3.2. Selección de medidas o técnica especial de investigación 644
3.3. Recolección de datos sobre la medida seleccionada 646
3.4. Indicación de mail para el envío del escrito 649
3.5. Envío de información a base de datos y procesamiento del sistema 651
3.6. Diagrama de flujo del sistema generado 653
4.0. Aclaraciones importantes 654
4.1. Términos Legales 654
4.2. Protección de datos personales 654
4.3. Envío de correo electrónico al usuario 656
5.0. Mejoras a futuro 657
5.1. Inclusión de más opciones de medidas o técnicas especiales de investigación 657
5.2. Mejoras en el desarrollo de sistema y diseño 659
5.4. Incorporación de inteligencia artificial 660
5.4.1. Procesamiento del lenguaje natural (NLP) 660
5.4.2. Generación de texto automática basado en legislación aplicable 660
5.4.3. Asistente virtual 660
5.4.4. Análisis predictivo 661
5.4.5. Personalización del servicio: 661
5.4.6. Detección de comportamientos dañinos 661
5.4.7. Mejora continua 661
5.5. Inclusión de normativa procesal penal aplicable 662
5.6. Mejoras a nivel de privacidad 662
6.0. Versión preliminar 1.0. 663
Guía de Buenas Prácticas para la solicitud de Medidas o Técnicas Especiales de Investigación para casos de Cibercrimen **664**
1.0. Aspectos Generales 664
1.1. Alcance 664
1.2. Finalidad 665
1.3. Principios aplicables 665
1.3.1. Principio de Excepcionalidad y Necesidad: 665
1.3.2. Principio de Especialidad: 665
1.3.3. Principio de Proporcionalidad: 666
1.3.4. Principio de razonabilidad: 666
2.0. De las medidas o técnicas especiales de investigación 666
2.1. Listado de medidas o técnicas especiales de investigación que no necesitan autorización judicial 666
2.1.1. Conservación inmediata de datos informáticos almacenados 667

2.1.1.1. ¿En qué consiste? 667
2.1.1.2. ¿Quién puede solicitar la medida? 667
2.1.1.3. ¿Qué límites deberían especificarse en la orden? 668
2.1.1.4. Notas adicionales 668
2.1.1.5. ¿Qué obtendría de esta solicitud? 668
2.1.1.6. Un ejemplo concreto del uso de esta medida o técnica especial de investigación 668
2.1.2. Identificación de dispositivo mediante captación de información de sistema 669
2.1.2.1. ¿En qué consiste? 669
2.1.2.2. ¿Quién puede solicitar la medida? 670
2.1.2.3. ¿Qué límites deberían especificarse en la orden? 670
2.1.2.4. Notas adicionales 670
2.1.2.5. ¿Qué obtendría de esta solicitud? 671
2.1.2.6. Un ejemplo concreto del uso de esta medida o técnica especial de investigación 671
2.1.3. Mandato de comunicación de datos de abonado 672
2.1.3.1. ¿En qué consiste? 672
2.1.3.2. ¿Quién puede solicitar la medida? 672
2.1.3.3. ¿Qué límites deberían especificarse en la orden? 673
2.1.3.4. Notas adicionales 673
2.1.3.5. ¿Qué obtendría de esta solicitud? 673
2.1.3.6. Un ejemplo concreto del uso de esta medida o técnica especial de investigación 673
2.2. Listado de medidas o técnicas especiales de investigación que necesitan autorización judicial 674
2.2.1. Mandato de comunicación de datos de tráfico y/o contenido 674
2.2.1.1. ¿En qué consiste? 674
2.2.1.2. ¿Quién puede solicitar la medida? 675
2.2.1.3. ¿Qué límites deberían especificarse en la orden? 675
2.2.1.4. Notas adicionales 675
2.2.1.5. ¿Qué obtendría de esta solicitud? 675
2.2.1.6. Un ejemplo concreto del uso de esta medida o técnica especial de investigación 676
2.2.2. Registro de datos informáticos almacenados (presencial con habilitación a remota) 676
2.2.2.1. ¿En qué consiste? 676
2.2.2.2. ¿Quién puede solicitar la medida? 677
2.2.2.3. ¿Qué límites deberían especificarse en la orden? 677
2.2.2.4. Notas adicionales 677
2.2.2.5. ¿Qué obtendría de esta solicitud? 678
2.2.2.6. Un ejemplo concreto del uso de esta medida o técnica especial de investigación 678
2.2.3. Interceptación de datos de tráfico y/o contenido 679
2.2.3.1. ¿En qué consiste? 679
2.2.3.2. ¿Quién puede solicitar la medida? 679
2.2.3.3. ¿Qué límites deberían especificarse en la orden? 680
2.2.3.4. Notas adicionales 680
2.2.3.5. ¿Qué obtendría de esta solicitud? 681
2.2.3.6. Un ejemplo concreto del uso de esta medida o técnica especial de investigación 681
2.2.4. Agente encubierto informático 682
2.2.4.1. ¿En qué consiste? 682
2.2.4.2. ¿Quién puede solicitar la medida? 682
2.2.4.3. ¿Qué límites deberían especificarse en la orden? 683

2.2.4.4. Notas adicionales 683
2.2.4.5. ¿Qué obtendría de esta solicitud? 684
2.2.4.6. Un ejemplo concreto del uso de esta medida o técnica especial de investigación 684
2.2.5. Registro Remoto 685
2.2.5.1. ¿En qué consiste? 685
2.2.5.2. ¿Quién puede solicitar la medida? 685
2.2.5.3. ¿Qué límites deberían especificarse en la orden? 686
2.2.5.4. Notas adicionales 686
2.2.5.5. ¿Qué obtendría de esta solicitud? 687
2.2.5.6. Un ejemplo concreto del uso de esta medida o técnica especial de investigación 687
3.0. Del sistema de generación de modelos de escritos de órdenes o solicitudes de medidas o técnicas especiales de investigación 687
3.1. Advertencias legales 687
3.2. Protección de Datos Personales 688
3.3. Acceso al sistema informático de la Guía 688
Bibliografía **689**

Agradecimientos:

Este trabajo de investigación, que se cristaliza en una tesis doctoral, no es un trabajo más. Se hace difícil escribir este apartado y soltar un trabajo que, durante los 10 años que ha llevado su realización, y como podrán observar en su lectura, conserva en sus venas parte de mi.

Es momento de agradecer. Y quiero dedicar estas primeras líneas a una persona fundamental en este camino de investigación: el Dr. José Benvenuti, de quien no puedo escribir sin llorar su pérdida tan reciente (Junio 2022). Semanas antes de su fallecimiento, me escribió por privado para comunicarme su orgullo por una conferencia que tuve la posibilidad de exponer, y en cuya ocasión le comenté que estaba preparando aspectos finales para presentar esta tesis, y que me gustaría que así como me entregó el diploma de abogado, me entregase en algún momento el diploma del doctorado, algo que acepto con el amor que siempre tuvo. Si bien eso ya no será posible, si es posible que esta dedicatoria quede inmortalizada para usted Dr. Benvenuti. Gracias por haberme enseñado el respeto y la sencillez como profesional, a ser buena persona primero y buen profesional después, a darle importancia no sólo a la investigación, sino también a su difusión y sobre todo, al aporte que debe generar en nuestra sociedad. Gracias.

Debo también expresar mi gratitud a algunas instituciones que hicieron posible este trabajo, sobre todo al Consejo Nacional de Investigaciones Científicas y Técnicas (CONICET), sin cuyo aporte, no hubiese sido posible dedicarme en los primeros años al Doctorado en Derecho. Asimismo, agradecer al Centro de Investigaciones de la Facultad de Ciencias Jurídicas y Sociales (UNL), donde pasé muchos años de mi vida.

Por último, y con mayor emoción, dedico esta tesis a mi familia, Marisa, Mario y Ricardo, por estar siempre. Por supuesto, para mi pareja Anita, por ser la inyección de amor y motivación que me acompañó en los últimos años de esta tesis. Gracias.

Introducción:

En la era de la información y la conectividad global, el avance tecnológico ha traído consigo no sólo innumerables beneficios, sino también desafíos sin precedentes para la seguridad cibernética y la integridad de sistemas digitales. El cibercrimen, una manifestación contemporánea de la delincuencia que explota la naturaleza virtual del mundo digital, ha evolucionado de manera exponencial, desafiando los marcos jurídicos y exponiendo las vulnerabilidades inherentes a la interconexión digital. En este contexto, el presente trabajo se sumerge en el análisis profundo y la comprensión de los desafíos jurídicos que el combate del cibercrimen implica en la actualidad.

La transformación digital y la expansión de las redes informáticas han revolucionado la forma en que las personas interactúan, las empresas operan y los gobiernos funcionan. Sin embargo, esta revolución tecnológica también ha dado paso a nuevas formas de criminalidad, donde los ciberdelincuentes explotan las lagunas legales y las debilidades de los sistemas de seguridad digital para llevar a cabo actividades ilícitas a una escala global y con una relativa impunidad. Desde el robo de información confidencial hasta el sabotaje de infraestructuras críticas y la propagación de malware, el cibercrimen se ha convertido en un desafío multifacético que trasciende fronteras y desafía los paradigmas tradicionales de persecución penal.

Este estudio reconoce que el combate del cibercrimen no puede limitarse exclusivamente a las soluciones técnicas, sino que requiere una aproximación interdisciplinaria que aborde sus complejas implicaciones legales, tecnológicas, sociales y éticas. A medida que las fronteras entre lo físico y lo digital se vuelven cada vez más difusas, los desafíos jurídicos emergen tanto en la definición de cibercrimen como en la obtención y presentación de pruebas en un entorno digital. Además, la cooperación internacional se convierte en un elemento crítico, ya que los delincuentes pueden operar desde cualquier parte del mundo, superando las limitaciones geográficas que tradicionalmente restringía la aplicación de la ley.

Siguiendo la línea de pensamiento del Profesor Melvin Kranzberg[1] consideramos pertinente considerar que si bien la tecnología no es buena ni mala, tampoco su uso -en sentido estricto- puede ser considerado neutral. Bajo este razonamiento, para poder encontrar una respuesta más adecuada, el observador deberá evaluar en cada momento como es que se está usando y quien la usa.

Los delitos informáticos representan para el Derecho una variada gama de desafíos y complicaciones, ya sean desde el punto de vista material como formal. Desde la facilidad para el anonimato en la red; el desdibujamiento de las fronteras para su comisión (trasnacionalidad); el aumento de usuarios con poco nivel de conocimiento informático (incremento de potenciales víctimas); así como la ausencia de herramientas jurídicas (materiales y procesales) adecuadas para su investigación y persecución, son algunos de los elementos que complejizan el combate contra la ciberdelincuencia y que intentaremos ir abordando en esta investigación.

A su vez, este tipo de delitos son también retroalimentados con la actividad en el mercado negro de la información, el cuál funciona como motor que impulsa una importante masa de ataques informáticos, principalmente destinados a obtener bases de datos con información personal y confidencial que luego se comercializan en la red.

Consideramos de gran importancia hacer un abordaje -al menos de una parte- de esa problemática, para en primer lugar comprender el fenómeno al cual nos enfrentamos, y en consecuencia, reflexionar puntualmente sobre si en la denominada Sociedad de la Información se afecta realmente la eficacia del derecho, y en su caso, hasta qué punto es necesario una adaptación o modificación de las reglas jurídicas que permitan disminuir las consecuencias negativas de los delitos informáticos.

El presente trabajo busca analizar en profundidad estos desafíos jurídicos, examinando cómo los marcos legales nacionales e internacionales están respondiendo al cibercrimen y cómo se están adaptando para abordar una realidad en constante evolución. Además, se explorarán las tensiones entre la necesidad de

[1] KRANZBERG, Melvin; “Technology and Culture”, Vol. 27, No. 3 (Jul., 1986), pp. 544-560

combatir el cibercrimen y el respeto a los derechos y libertades individuales en el mundo digital.

A través de un enfoque interdisciplinario que incorpora aspectos de derecho penal, derecho internacional, ciberseguridad y tecnología, esta tesis de doctorado pretende contribuir al entendimiento de los desafíos actuales y futuros en la lucha contra el cibercrimen y a la formulación de soluciones efectivas y equitativas en este complejo escenario legal y tecnológico.

1.1. Objeto y tesis propuesta

El presente trabajo intenta inicialmente exponer las relaciones que existen entre las distintos escenarios jurídicos relacionados a los delitos informáticos y su persecución, en particular, sobre la potencial afectación a los derechos de las personas que puede darse en el marco del despliegue de distintas medidas y herramientas de investigación tendiente a combatir los delitos informáticos y el cibercrimen.

Entendemos que esta empresa es importante, toda vez que podría ser utilizada como un parámetro para comprender el rol tiene el Estado sobre esta problemática social y sobre todo, si es posible encontrar un equilibrio entre la construcción y regulación de medidas de investigación que tiendan a mejorar la eficacia en la persecución de los delitos informáticos, sin que las mismas implican, tanto a nivel nacional como internacional, en la afectación de derechos y garantías de las personas.

Desde esta perspectiva se ha seleccionado como caso de estudio a los delitos informáticos, como un fenómeno novedoso -o no tan novedoso como ya veremos- cuyas raíces y consecuencias tecnológicas implican para el Derecho una compleja lista de desafíos y obstáculos, que pretendemos ir descubriendo a lo largo de este trabajo.

Se propone entonces en una primera etapa realizar un análisis y cotejo de las normativas tanto de fondo como de forma entre Argentina, Brasil, Colombia, México y España.

Consideramos de interés realizar un estudio sobre los niveles de coordinación en algunos países latinoamericanos (más representativos a nivel de población) de las políticas legislativas penales en relación a los delitos informáticos bajo el razonamiento que la problemática no puede entenderse como local, sino que por sus características propias, hace que el delito informático pueda ser cometido desde cualquier lugar.

En una segunda etapa, buscaremos avanzar en miras a comparar el nivel de regulación en materia procesal penal de los países del estudio, en relación con el Convenio de Cibercrimen de Budapest (CE) y el Proyecto de la Convención Internacional Integral sobre la Lucha contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos (ONU).

Generado todo el cuadro de cumplimiento y teniendo el marco teórico adecuado para realizar la comprobación de las hipótesis de trabajo, consideramos que tendremos el escenario adecuado para avanzar hacia la tercera y última etapa de este trabajo: la generación de la tesis o propuesta.

Nuestra tesis consiste en la propuesta de una **"Guía de Buenas Prácticas sobre medidas o técnicas especiales de investigación para el cibercrimen",** que incluya un listado de medidas o técnicas especiales de investigación, no ya desde un punto de vista de sugerencia normativa (como podría ser la búsqueda de instrumentos internacionales como el Convenio de Budapest), sino desde un punto de vista más práctico, orientado hacia la descripción, solicitud y sobre todo, la necesidad de controles y límites jurisdicciones que deberían ser tenidos en cuenta para que dichas medidas de injerencia sean lo menos riesgosas posibles para los derechos y libertades de las personas.

Entendemos que esta guía de buenas prácticas implicaría un aporte en materia procesal penal, que iría acompañada de la propuesta de un sistema informático, que automatiza la recepción de los casos, generando a pedido, los modelos o plantillas de los pedidos de autorización (o en algunos casos, de la propia medida de investigación) a fin de facilitar el acceso a dichos recursos a todas aquellas jurisdicciones que aún no poseen avances en dicho campo.

La construcción de esta guía, tendrá en cuenta toda la información aprendida a lo largo de la tesis, buscando unificar en un sistema informático propuesto, las

mejores prácticas relevadas de los distintos sistemas alcanzados por el estudio. Claro está, que dichas propuestas no serán obligatorias ni vinculantes, pero nuestro deseo es que sean útiles como referencia internacional, en aras de la generación de un consenso común que siempre tenga sobre el horizonte, minimizar la potencial afectación a los derechos de las personas que puede darse en el marco del despliegue de distintas medidas y herramientas de investigación tendiente a combatir los delitos informáticos y el cibercrimen.

1.2. Situación problemática

La situación problemática general parte de considerar que el actual sistema normativo vigente en Argentina, a nivel estadístico, es insuficiente para garantizar una detección, investigación y sanción eficaz de los delitos informáticos.

Si bien esta problemática no podría ser considerada como exclusiva de Argentina, toda vez que al igual que en otras áreas de delincuencia compleja (narcotráfico, trata de personas, etc.), existen informes internacionales[2] que desde hace años vienen anunciando la necesidad de trabajar en la materia, reconociendo la magnitud de la problemática.

En consecuencia, la ciberdelincuencia es en sí misma una situación problemática social en crecimiento, que a nuestro criterio merece de un estudio minucioso y detallado que permita, en principio, comprender el fenómeno, y posteriormente repensar al derecho como herramienta que permita avanzar en la mitigación o combate del mismo.

Como señala el Dr. Pablo Palazzi[3], uno de los referentes en la materia a nivel internacional, “el delito informático ya no puede ser ignorado por el legislador: su realidad y su presencia son incontrolables y sus efectos pueden ser realmente

[2] NACIONES UNIDAS, New York, 2013. UNODC. Comprehensive Study on Cybercrimen. Url: http://www.unodc.org/documents/organizedcrime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf. Consultado: 27 de Noviembre de 2019

[3] PALAZZI, P., “Los delitos informáticos en el Código Penal. Análisis de la ley, 26388”, Editorial Perrot, A. (2016).

devastadores. Basta citar los millones de dólares en daños y pérdidas que ocasionan los virus informáticos, o las estafas por esa vía, o para citar un fenómeno más común, el ataque mediante denegación de servicios que lleva incluso a prácticas extorsivas de ofrecimientos de seguridad a las empresas en internet".

Participamos de creer que la situación actual en la materia se presenta como grave no sólo por sus consecuencias negativas directas en la sociedad (afectación a los bienes jurídicos), sino que a la postre, la inexistencia de consecuencias penales a los autores de los delitos, generan en la sociedad una -lógica y razonable- pérdida de confianza en la justicia.

Por ello, a través de la metodología de trabajo planteada en este estudio, se pretende hacer una abordaje de las fuentes de esta problemática, a fin de buscar comprender sus raíces y desde allí brindar un aporte útil para lograr que en nuestro país se pueda avanzar con destino a un marco jurídico desarrollado y apto para combatir la ciberdelincuencia.

1.3. Construcción de Hipótesis y Objetivos

1.3.1. Hipótesis a validar

La hipótesis del presente estudio, que será analizada y confrontada a lo largo del desarrollo del trabajo, a fin de concluir en su sustentabilidad o no, parte de la siguiente premisa:

- *A nivel de normativa penal material, Argentina, Brasil, Colombia, México y España han adecuado sus ordenamientos jurídicos de acuerdo a lo sugerido por el Convenio de Budapest (art. 2 a 9) y por el Proyecto de la Convención Internacional Integral sobre la Lucha contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos (art. 6 a 16).*
- *A nivel de normativa procesal penal, Argentina, Brasil, Colombia, México no han adecuado sus ordenamientos jurídicos para regular las medidas o técnicas especiales de investigación sugeridas por el Convenio de Budapest*

(art. 16 a 21) y el Proyecto de la Convención Internacional Integral sobre la Lucha contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos (art. 25 a 30). España es el único país de los incluídos en el estudio que se encontraría en cumplimiento.

1.3.2. Objetivos Específicos para validación de hipótesis

Para poder avanzar en la comprobación o refutación de dichas hipótesis, se propone avanzar sobre los objetivos específicos:

1. Identificar la normativa de tipos penales vigentes sobre delitos informáticos en los distintos ordenamientos jurídicos de Argentina, Brasil, Colombia, México y España.
2. Paragonar los delitos informáticos tipificados (previa elección de los delitos alcanzados) en los distintos ordenamientos jurídicos incluídos en el estudio y compararlos con los instrumentos internacionales de lucha contra el cibercrimen.
3. Abordar el marco teórico necesario para determinar la necesidad de regulación de medidas o técnicas especiales de investigación sobre delitos informáticos y su relación con la efectiva o potencial afectación al respeto a los derechos y libertades individuales del ámbito digital que implican.
4. Identificar la normativa procesal penal destinada a la obtención de evidencia digital en los distintos ordenamientos jurídicos de Argentina, Brasil, Colombia, México y España.
5. Paragonar las medidas de investigación destinadas a la obtención de evidencia digital reguladas (previa elección de los medidas de investigación alcanzadas) en los distintos ordenamientos jurídicos incluídos en el estudio y compararlas con los instrumentos internacionales de lucha contra el cibercrimen.
6. En base a las conclusiones alcanzadas, proponer y generar un Guía de Buenas Prácticas para la solicitud de Medidas o Técnicas Especiales

de Investigación para casos de Cibercrimen que tenga por finalidad brindar una guía marco para fuerzas de seguridad y Ministerios Públicos Fiscales que no tengan legislación aplicable en la materia, teniendo siempre en cuenta la debida garantía de los derechos humanos y las libertades de las personas.

1.3.3. Objetivos Generales

A su vez, desde una perspectiva más general se proponen como objetivos generales de la investigación:

1. Generar avances en el ámbito de la teoría socio-jurídica sobre el tratamiento de los delitos informáticos desde la óptica del derecho procesal penal en Argentina.
2. Contribuir al desarrollo de un enfoque técnico-jurídico como base para fomentar una mejora en el sistema de regulación de los delitos informáticos en Argentina, tendiendo a alcanzar políticas penales internacionales y comunes destinadas a proteger a la sociedad de la ciberdelincuencia.
3. Aportar al desafío de la investigación de los delitos informáticos una Guía o Manual que proponga al menos preliminarmente, un abanico de medidas de investigación que podrían ser utilizadas en el marco de la identificación, persecución y condena del cibercrimen.

1.4. Antecedentes personales

En relación con los antecedentes personales relacionados a la propuesta, vale destacar que la presente línea de trabajo es un anhelo construido por varios años de trabajo en temáticas relacionadas, como es la Seguridad de la Información.

El genuino interés de este autor ha venido desarrollándose a través de la realización de diferentes estudios e investigaciones preliminares que intentaron

abordar pequeños fragmentos del saber en materia de delitos informáticos[4], pero que hoy en día conceden un aporte a la generación de los objetivos planteados en este plan de trabajo.

Así se comenzó a analizar al acceso indebido[5] (*hacking)* como uno de los delitos informáticos que podían llegar a comprometer la privacidad de los usuarios dentro del ámbito privado de una organización. En ese mismo año, se avanzó sobre el estudio de otro fenómeno en crecimiento: el *Phishing* o captación ilegítima de datos confidenciales[6], en el cuál se hizo un análisis crítico sobre el funcionamiento del art. 173 inc. 16 (incorporado a través de la Ley Nº 26.388) y su dudosa capacidad de tipificación de las conductas conocidas como *phishing*[7].

A consecuencia de la postura crítica expresada en dicho artículo, y a solicitud de asesores de la Senadora Nacional María de los Ángeles Higonet, se ha tenido la posibilidad de realizar una investigación especial durante el año 2011, con destino en la redacción de un proyecto de Ley para la incorporación de un nuevo delito informático que considere como delito a la conducta del *phishing* en Argentina. Dicho proyecto fue finalmente presentado en el Honorable Congreso de la Nación[8] y defendido oportunamente ante la Comisión de Justicia y Asuntos Penales.

---

[4] TEMPERINI, Marcelo, "Internet y Privacidad en las Empresas: entre Políticas, Delitos y Garantías Constitucionales en Argentina". Publicada en el Simposio de Informática y Derecho. Jornadas Argentinas de Informática Nº 38. ISSN 1850-2814.

[5] TEMPERINI, Marcelo, "Delitos Informáticos: La punibilidad del Hacking y sus consecuencias". Publicado en el Simposio de Informática y Derecho. Jornadas Argentinas de Informática Nº 39. ISSN 1850-2814

[6] TEMPERINI, Marcelo, "Phishing: Tipo penal en Argentina y sus consecuencias". Publicado en el Blog de Seguridad de la Información Segu-Info. Url: http://blog.segu-info.com.ar/2011/02/phishing-tipo-penal-en-argentina-y-sus.html

[7] TEMPERINI, Marcelo y BORGHELLO Cristian, "La captación ilegítima de datos confidenciales como delito informático en Argentina". Publicada en el Simposio de Informática y Derecho. Jornadas Argentinas de Informática Nº 41. ISSN: 1850-2814.

[8] HONORABLE SENADO DE LA NACIÓN ARGENTINA, Proyecto de Ley Nº 2257/11 "Proyecto de Ley incorporando el Art. 157 ter al Código Penal, tipificando el delito de obtención ileígtima de datos personales (phishing). Url: http://www.senado.gov.ar/web/proyectos/verExpe.php?origen=S&tipo=PL&numexp=2257/11&nro_comision=&tConsulta=2

A principios de 2012, el mismo grupo de asesores del Senado de la Nación ha solicitado la realización de una segunda investigación para la redacción de otro proyecto de Ley en materia de Delitos Informáticos, sobre la viabilidad en la propuesta de un tipo penal que pueda sancionar la Suplantación de Identidad Digital, otra de las conductas socialmente disvaliosas que existen en las redes y que actualmente no poseen sanción en Argentina. Este último proyecto fue realizado[9] fue presentado en el Honorable Congreso de la Nación[10] en fecha 15 de Mayo de 2012.

A partir de Abril de 2013, ya en el marco de la Beca de Doctorado de CONICET, se ha avanzando hacia un estudio aún mucho más profundo sobre la materia, comenzando con un estudio sobre los diferentes tipos de ataques informáticos de los cuáles es víctima la propia Administración Pública Nacional[11] -entre ellos, algunos sitios vinculados al propio CONICET-.

En el año 2015, en el contexto de nuestra participación en el Centro de Investigaciones de la Facultas de Ciencias Jurídicas y Sociales de la Universidad Nacional del Litoral, hemos aportado un artículo a la Revista "Papeles del Centro", describiendo parte de la complejidad de nuestro tema de especialización[12].

Durante el 2016, hemos generado un aporte de mucho interés, dedicado al abordaje de la Deep web, el anonimato y su relación con el Cibercrimen[13], publicada en el VI Congreso Iberoamericano de Investigadores y Docentes de Derecho e

---

[9] TEMPERINI, Marcelo y BORGHELLO, Cristian, "Suplantación de Identidad Digital como delito informático en Argentina". Publicada en el Simposio de Informática y Derecho. Jornadas Argentinas de Informática Nº 41. ISSN: 1850-2814.

[10] HONORABLE SENADO DE LA NACIÓN ARGENTINA, Proyecto de Ley Nº 1312/12 "Proyecto de Ley incorporando el Art. 138 bis al Código Penal, tipificando el delito de Suplantación de Identidad Digital". Url: http://www.senado.gov.ar/web/proyectos/verExpe.php?origen=S&tipo=PL&numexp=1312/12&nro_comision=&tConsulta=1

[11] TEMPERINI, Marcelo y BORGHELLO, Cristian, "Ciberseguridad Nacional Argentina: Cracking de Servidores de la Administración Pública". Publicado en el Simposio de Informática y Derecho. Jornadas Argentinas de Informática Nº 42. ISSN: 1850-2814. Año 2013.

[12] TEMPERINI, Marcelo: "El desafío de la lucha contra el Cibercrimen en Argentina". Publicado en Papeles del Centro de Investigaciones, Facultad de Ciencias Jurídicas y Sociales, UNL, publicación semestral, año 5, número 16, Santa Fe, República Argentina, 2015, pp. 31–51. ISSN 1853-2845

[13] TEMPERINI, Marcelo: "Deep web, anonimato y cibercrimen" - VI Congreso Iberoamericano de Investigadores y docentes de derecho e informática (CIIDDI 2016) - ISBN: 9789876921381 - 2016

Informática (CIIDDI 2016), organizado por la Red CIIDDI, la Facultad de Ciencias Jurídicas y Sociales y la Facultad de Ingeniería y Ciencias Hídricas de la Universidad Nacional del Litoral.

En el año 2017 hemos participado de la publicación del libro "Cibercrimen: aspectos de Derecho penal y procesal penal. Cooperación internacional. Recolección de evidencia digital. Responsabilidad de los proveedores de servicios de internet", dirigido por la Fiscal Daniela Dupuy. En dicha ocasión, hemos participado con dos artículos. Uno dedicado a nuevas herramientas de investigación penal, en particular trabajando el instituto del Agente Encubierto Digital[14]. El otro artículo, fue realizado en coautoría con el Lic. Cristian Borghello, abordando el tratamiento de la Suplantación de Identidad Digital como delito informático[15].

En el año 2018, hemos generado una investigación dedicada a cubrir aspectos esenciales de la temática del cibercrimen, trabajando alcances, conceptos y características, publicado en la editorial Erreius[16].

En el año 2019, hemos formado parte de la publicación del libro "Cibercrimen II: Nuevas conductas penales y contravencionales. Inteligencia artificial aplicada al Derecho penal y procesal penal. Novedosos medios probatorios para recolectar evidencia digital. Cooperación internacional y victimología.", dirigido por la Fiscal Daniela Dupuy. En dicha ocasión, hemos colaborado con un artículo dedicado a Técnicas y tendencias de investigación penal y su afectación a los derechos constitucionales[17].

---

[14] TEMPERINI, Marcelo; MACEDO, Maximiliano: "Nuevas herramientas de investigación penal: el Agente Encubierto Digital"; Libro Cibercrimen: aspectos de Derecho penal y procesal penal. Cooperación internacional. Recolección de evidencia digital. Responsabilidad de los proveedores de servicios de internet". Directora: Daniela Dupuy; Editorial: Editorial B de f; 2017. ISBN: 978-997-474-506-3.

[15] TEMPERINI, Marcelo; BORGHELLO, Cristian: "Suplantación de Identidad Digital como delito informático". Libro Cibercrimen: aspectos de Derecho penal y procesal penal. Cooperación internacional. Recolección de evidencia digital. Responsabilidad de los proveedores de servicios de internet". Directora: Daniela Dupuy; Editorial: Editorial B de f; 2017. ISBN: 978-997-474-506-3.

[16] TEMPERINI, Marcelo: "Delitos informáticos y cibercrimen: alcances, conceptos y características"; Libro "Cibercrimen y delitos informáticos : los nuevos tipos penales en la era de internet", Editorial Erreius 2018, ISBN: 978-987-4405-56-2

[17] TEMPERINI, Marcelo: "Técnicas y tendencias de investigación penal y su afectación a los derechos constitucionales", Cibercrimen II: Nuevas conductas penales y contravencionales. Inteligencia artificial

En el año 2020, hemos formado parte de la publicación del libro "Protección de datos. Doctrina y jurisprudencia", tomos 1 y 2, editada por Pablo A. Palazzi y el CETYS, a través de la colaboración con el artículo dedicado a "OSINT: Legalidad y protección de datos personales"[18].

Al momento de la finalización de la presente tesis, el autor se encuentra cubriendo cargos como profesor en las siguientes instituciones:

- Capacitador y asesor durante más de 5 años en el Ministerio Público de la Acusación de la Provincia de Santa Fe, en materia de Investigación, Buenas Prácticas en identificación, recolección y preservación de prueba informática.
- Capacitador y asesor en distintas fuerzas de seguridad federales y provinciales de Argentina, en materia de investigación del delito a través de nuevas tecnologías y recolección de evidencia digital.
- Capacitador y asesor en buenas prácticas de recolección y adquisición de Evidencia Digital en los Colegios de Escribanos de distintas jurisdicciones (Santa Fe, Mendoza, Chaco, Misiones, entre otros).
- Profesor en el Curso Avanzado "Prueba Digital: Identificación, recolección y preservación", organizado y certificado por la Universidad Notarial Argentina.
- Profesor en el Curso organizado por el Consejo Federal del Notariado Argentino, exponiendo sobre "Aspectos Procesales de las Pruebas Informáticas".
- Profesor en la Diplomatura en Análisis Forense Digital, organizada por la Universidad del CEMA, dictando el Módulo "Prueba Informática: Admisibilidad y valor probatorio"
- Profesor en la Diplomatura "Ciberdelitos y Evidencia Digital", organizada por la Universidad Católica (UCA Rosario), en el Módulo "Impugnación de Evidencia Digital"

aplicada al Derecho penal y procesal penal. Novedosos medios probatorios para recolectar evidencia digital. Cooperación internacional y victimología.". Directora: Daniela Dupuy; Editorial: Editorial B de f; 2019. ISBN: 978-9974-745-64-3.

[18] TEMPERINI, Marcelo y MACEDO, Maximiliano; "OSINT: Legalidad y protección de datos personales"; Libro "Protección de datos. Doctrina y jurisprudencia. Tomos 1 y 2." Compilador: Pablo Palazzi. Editorial CDYT. 2021

- Profesor en la Diplomatura “Cibercrimen y Evidencia Digital”, organizada por la Universidad de Champagnat (UCH Mendoza), en el Módulo de “Legalidad en Pericias Informáticas”.
- Profesor en el Posgrado de Derecho Procesal Penal, organizado por la Facultad de Ciencias Jurídicas y Sociales de la Universidad Nacional del Litoral, dictando clases especiales sobre “Medidas de investigación, Evidencia Digital y Garantías constitucionales”
- Profesor en el Posgrado Iberoamericano de Cibercrimen, organizada por el Instituto Argentino de Reconstrucción Forense Especializada, en tema de “Herramientas innovadoras para investigar”.
- Profesor en la Certificación en Ciberseguridad “Fundamental of hacking & defense”, organizada por Hackademy de Ekoparty, en el Módulo “Ethics, Law & Cybercrime”.
- Profesor del módulo de “Pericias Informáticas” en el Posgrado de Medicina Legal de la Universidad Nacional del Litoral.
- Profesor en el Curso de Actualización en Cibercrimen, Delitos Informáticos y Evidencia Digital, organizado por la Secretaría de Posgrado de la FCJS – UNL.
- Profesor invitado en la Asociación Argentina del Derecho del Trabajo y de la Seguridad Social, exponiendo sobre “¿Cómo aportar prueba informática de forma válida en el proceso judicial?”

Como se puede observar, existen serios antecedentes sobre una labor previa en el tema propuesto, demostrando un real interés en su estudio e investigación. Además, se encuentra reforzado por proyectos y trabajo en materia informática y de Seguridad de la Información, líneas del saber que brindan conocimientos básicos y necesarios para una mejor comprensión y desarrollo de la problemática, fomentando la articulación de los saberes jurídicos y los saberes científico-tecnológicos que movilizan los cambios en la regulación sobre delitos informáticos en Argentina.

1.5. Metodología y marco conceptual

Tanto en la primera etapa relacionada con el estudio sobre la situación de derecho penal material, como en una segunda etapa sobre el estudio de la situación en procesal penal de los países incluídos en el estudio se considera que la mejor estrategia teórico-metodológica será la de tipo cualitativo, en especial siguiendo el modelo jurídico analítico y comparativo.

De esta forma se realizará el abordaje inicial de los sistemas normativos penales de fondo de los países alcanzados en el estudio, y posteriormente, un análisis sobre las regulaciones en materia procesal y sus niveles de adecuación a los instrumentos internacionales en la materia.

En cuanto a la metodología analítica, en la primera etapa se aplicará en el estudio de las normas jurídicas, en especial del derecho comparado, sumado a un análisis e interrelación de distintos artículos doctrinarios, así como publicaciones e informes oficiales, tanto a nivel nacional como internacional. Adicionalmente, se complementará con la participación en congresos, jornadas, seminarios, así como en la divulgación de resultados, presentación de publicaciones, entre otros, que conformarán el desarrollo metodológico de la presente investigación.

Desde el punto de vista temporal, el diseño será sincrónico (no diacrónico).

Capítulo I: La eficacia del Derecho en los delitos Informáticos

1.1. Introducción

Las nuevas tecnologías han acelerado muchos procesos de cambios sociales. La velocidad y las posibilidades que se brindan a través de las nuevas herramientas de la información y las comunicaciones tienen la potencialidad de generar, modificar o alterar conductas sociales que tienen consecuencias directas e indirectas sobre una de las más importantes funciones del Derecho: el control social.

En este marco, algunas de las características propias de esta nueva Sociedad de la Información, tales como la comunicación global desde y hacia cualquier lugar del mundo, la posibilidad de realización de acciones masivas con tan sólo un par de clicks, y sobre todo, la posibilidad de un gran nivel de anonimato, representan una serie de complicaciones para el derecho en general, y para su eficacia en el derecho penal en particular.

El presente capítulo es a título introductorio del trabajo planteado, donde se propone como objeto de estudio el análisis y reflexión sobre si esta nueva (o no tan nueva) Sociedad de la Información afecta la eficacia del derecho en general y en su caso, hasta qué punto es necesario una adaptación o modificación de las reglas jurídicas.

De sus conclusiones preliminares, podremos avanzar sobre una primera aproximación sobre si las hipótesis de trabajo planteadas sobre los delitos informáticos es exclusiva del derecho penal, o bien, podría pensarse que la Sociedad de la Información también ha traído consecuencias para otras ramas del Derecho.

1.2. El Derecho y su función de control social

Dentro de una serie de importantes autores bautizados como *funcionalistas*, se considera que una de las principales funciones del derecho es la de ejercer el "control social", entendiendo que el mismo opera integrando los comportamientos sociales en un modelo normativo establecido y corrigiendo o reprimiendo las posibles conductas "desviadas" de algunos de sus integrantes.

Siguiendo la línea de Parsons y Durkheim, es a través de este control social que se puede accionar frente a las "conductas desviadas" –consideradas como fallos ocasionales y transitorios en el proceso de socialización-, siendo entonces "*el Derecho un tipo de control represivo y a posteriori, mediante el cual se permite reafirmar los valores protegidos por el sistema, que son los que realmente mantienen la cohesión y el orden social*". [19]

Desde esta postura doctrinaria, se sostiene que en cualquier tipo de control social es necesario la presencia de dos elementos: el material y el formal. En el primero de ellos, dentro del aspecto material, encontramos a su vez los elementos normativos y valorativos de la conducta que se quieren transmitir a los individuos con la finalidad de orientar e integrar socialmente sus comportamientos. En el segundo elemento, el formal, se observan en cambio los mecanismos, técnicas e instrumentos a través de las cuáles se transmiten las pautas de comportamientos a los individuos, siendo el ejemplo clásico para este aspecto, el uso de la fuerza por parte del Estado.

Destacamos este último elemento del control social, el formal, el cuál será de utilidad al momento de plantear la reflexión pretendida en el presente trabajo.

[19] PECES-BARBA, Gregorio; FERNANDEZ, Eusebio; DE ASIS, Agustin; "Curso de Teoría del Derecho". Ed. Marcial Pons, 1999, Madrid.

1.3. La Eficacia como valor en el Derecho

En el marco de la teoría de la norma jurídica, desde hace tiempo la doctrina más calificada y autorizada ha estudiado los distintos problemas clásicos, muchos aún en discusión hasta la actualidad. Entre ellos, el maestro Norberto Bobbio, es quien reconoce que toda norma jurídica puede ser sometida a tres distintas valoraciones, independientes entre sí:

- si la norma es justa o injusta;
- si la norma es válida o inválida,
- si la norma es eficaz o ineficaz.

Como oportunamente se expresó, el presente trabajo pretende tomar sólo una de estas valoraciones, la eficacia del derecho, a fin de ser analizada a la luz de los cambios que implica la sociedad de la información.

De acuerdo al profesor Bobbio, el abordaje sobre la eficacia de una norma implica "*el problema de si la norma es o no cumplida por las personas a quienes se dirige (los llamados destinatarios de la norma jurídica) y, en el caso de ser violada, que se la haga valer con medios coercitivos por la autoridad que la ha impuesto. Que una norma exista en cuanto norma jurídica, no significa que también sea constantemente cumplida*"[20].

1.4. Otros conceptos de eficacia

Una diferente concepción a la ensayada sobre la eficacia en el Derecho puede ser observada en la obra del histórico maestro positivista Hans Kelsen, quien conforme a su teoría pura, el derecho es un conjunto de normas o un orden normativo, donde la diferencia entre Derecho y otros órdenes sociales es que el derecho es un orden coercitivo.

En la concepción de su sistema, si un individuo está jurídicamente obligado a comportarse de cierta manera en relación con otro, este segundo tiene un derecho a

[20] BOBBIO, Norberto. "Teoría General del Derecho"; 2da. Edición, Editorial Temis, 1994.

la conducta del primero. En palabras de este autor "*Un orden jurídico como un todo, y las normas jurídicas particulares que constituyen este orden jurídico, se consideran válidas si son, en todos los ámbitos, obedecidas y aplicadas, o sea, si tienen eficacia. La validez significa que la ley debe ser obedecida y aplicada; la eficacia quiere decir que la ley es, en verdad, obedecida y aplicada.*"[21]

En su obra Teoría General del Derecho y del Estado[22], Kelsen desarrolla con mayor profundidad su concepto y relación dependiente entre validez y eficacia, afirmando que el hecho que "*la validez de un orden jurídico dependa de su eficacia no implica, según hemos dicho, que la validez de una norma aislada sea dependiente de su efectividad. La norma jurídica aislada permanece válida mientras forma parte de un orden válido. El problema de determinar si una norma aislada es válida, se resuelve recurriendo a la primera Constitución. Si esta tiene validez, entonces todas las normas que han sido constitucionalmente creadas son igualmente válidas. El principio de efectividad implícito en el derecho internacional refiérese inmediatamente sólo a la primera Constitución de un orden jurídico nacional, y por tanto, únicamente se refiere a este orden considerado como totalidad. Tal principio puede, sin embargo, ser también adoptado en cierta medida por el derecho nacional, y, de este modo, la validez de una norma aislada dentro del orden jurídico nacional se puede hacer depender de su eficacia. Es este el caso en que se admite la posibilidad de que una norma jurídica pierda su validez por desuso.*"

Otro de los grandes autores con palabra autorizada sobre la temática como Herbert Hart refiere también a la relación entre validez y eficacia en el Derecho. De acuerdo a un estudio realizado por la Dra. Cristina Fuertes-Planas Aleix[23], para Hart la eficacia de un orden jurídico consiste en el hecho de que generalmente los individuos a quienes se dirigen las normas se conforman con ellas y en caso de incumplimiento, se aplican también generalmente las sanciones previstas para tales

[21] KELSEN, Hans; Bulygin, Eugenio. "Validez y eficacia del Derecho". Ed. ASTREA, 2005.

[22] KELSEN, Hans, "Teoría general del derecho y del Estado", Imprenta Universitaria, México, D. F., 1949.

[23] FUERTES-PLANAS ALEIX, Cristina; "Validez, obligatoriedad y eficacia del derecho en H. L. A. Hart", Anuario de Derechos Humanos. Nueva Época. Vol. 8. 2007 (131-186). España.

supuestos. En primer lugar, hace referencia a la conexión entre validez y eficacia respecto de normas jurídicas singulares, en cuyo caso expresa que no hay conexión necesaria entre la validez de la norma particular y su eficacia, "*salvo que la regla de reconocimiento del sistema incluya entre sus criterios, como algunas lo hacen, la provisión (algunas veces llamada regla de desuso) de que ninguna regla ha de valer como regla del sistema si hace mucho que ha dejado de ser eficaz*".

Es decir, que la misma regla de reconocimiento incluya como uno de sus criterios de validez la afirmación de que no puede haber norma válida que no sea eficaz. Sin embargo, existe una estrechisima vinculación entre validez y eficacia de las normas jurídicas particulares, ya que una persona que hace un enunciado interno referente a la validez de una norma particular de un sistema presupone -dice Hart- la verdad del enunciado fáctico externo de que el sistema es generalmente eficaz, porque el uso normal de enunciados internos se produce en un contexto de eficacia general.

1.5. Eficacia: grados y metodología.

Si bien sería posible citar otras tantas definiciones y conceptos sobre la eficacia en el derecho, nos limitaremos a las ya realizadas, en ocasión de la brevedad y objetivos buscados en el presente capítulo. De los conceptos expuestos, adoptaremos el expresado por Bobbio[24], quien, a paso siguiente de su conceptualización, procede a determinar distintos grados o categorías de eficacia en las normas:

Normas	Nivel de Eficacia
Aquellas que son cumplidas universalmente de manera espontánea	Las más eficaces

[24] BOBBIO, Norberto. "Teoría General del Derecho"; 2da. Edición, Editorial Temis, 1994.

Aquellas que se cumplen por lo general solo cuando van acompañadas de coacción	Eficaces
Aquellas que no se cumplen a pesar de la coacción	Ineficaces
Aquellas que incluso ante su violación, tampoco se aplica coacción	Las más ineficaces

En búsqueda de avanzar en el estudio de la eficacia y su importancia en la función del derecho, sostiene Bobbio que mientras la investigación sobre la justicia de la norma es de carácter filosófico; la investigación sobre la validez es típicamente jurídica, la investigación para determinar la eficacia o ineficacia de una norma es más bien de carácter histórico-social, orientándose al estudio del comportamiento de los miembros de un determinado grupo social.

Sostiene entonces que se puede afirmar que el problema de la eficacia de las reglas jurídicas es el problema fenomenológico del derecho. Es decir, intentar determinar la eficacia o ineficacia de una norma, inevitablemente nos involucra en "*el terreno de la aplicación de las normas jurídicas, o sea al terreno de los comportamientos efectivos de los hombres que viven en sociedad, de sus intereses opuestos, de las acciones y reacciones frente a la autoridad, y da lugar a las investigaciones en torno a la vida del derecho, en su nacimiento, en su desarrollo, en sus cambios, investigaciones que de ordinario están relacionadas con el análisis de carácter histórico y sociológico. De aquí nace el aspecto de la filosofía del derecho que lleva a la sociología jurídica*"[25].

En conclusión, intentar develar los niveles de eficacia de una norma, nos obliga a la necesidad de medir los comportamientos efectivos del hombre en sociedad, para determinar su decisión frente a la norma, de respeto y seguimiento (eficacia), o bien de ignorancia e infracción a las obligaciones establecidas (ineficacia).

[25] BOBBIO, Norberto. "Teoría General del Derecho"; 2da. Edición, Editorial Temis, 1994.

1.6. La Era de la Sociedad de la Información

Desde la UNESCO[26] se ha llevado a cabo la Cumbre Mundial de la Sociedad de la Información[27] (CMSI), la cuál tuvo lugar en dos fases: la primera fue realizada del 10 al 12 de diciembre de 2003, en Ginebra (Suiza), donde se adoptó una declaración de principios y un plan de acción. La segunda fase se llevó a cabo del 16 al 18 de noviembre de 2005 en Túnez. En ambas fases, se manifiesta el compromiso de construir una sociedad de la información centrada en la persona, en donde todos puedan crear, consultar, utilizar y compartir la información y el conocimiento, elevando así la calidad de vida de los pueblos, sobre la base de la Declaración Universal de los Derechos Humanos.

Numerosos conceptos y desarrollos pueden encontrarse en la actualidad sobre lo que es la Sociedad de la Información, o para algunos, Sociedad del Conocimiento. Entre ellos, nos parece adecuada la descripción realizada por Rodolfo Herrera Bravo, quien expresa al respecto que "*Detrás de todo este desarrollo tecnológico descansa la información como objeto de dicha revolución. La información ya era valiosa en el pasado, significaba encontrarse en una situación ventajosa respecto a quienes no la tenían. Pero en el presente su valor se acrecienta, ya que antes no existía la posibilidad de convertir informaciones parciales y dispersas en informaciones en masa y organizadas, de interrelacionar esa información y de procesarla con rapidez, como ocurre hoy, en la sociedad de la información. En definitiva, lo que ocurre es que esa información cada vez aporta más conocimiento, que es lo verdaderamente importante, y que quien dispone de conocimiento tiene poder*"[28]

Entre los numerosos principios que se han expresado en la CMSI, se reafirma como fundamento esencial de la Sociedad de la Información, y según se estipula en

[26] Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO)

[27] CUMBRE MUNDIAL DE LA SOCIEDAD DE LA INFORMACIÓN; WSIS-03/GENEVA/4-S; 12 de mayo de 2004; Url: http://www.itu.int/wsis/docs/geneva/official/dop-es.html, Consultado: : 10 de Abril de 2014

[28] HERRERA BRAVO, Rodolfo. "El Derecho en la Sociedad de la Información: Nociones generales sobre el Derecho de las Tecnologías de la Información y las Comunicaciones.", Publicado en DerechoTecnologico.com, Url: http://www.derechotecnologico.com/estrado/estrado002.html

el Artículo 19 de la Declaración Universal de Derechos Humanos, que "*todo individuo tiene derecho a la libertad de opinión y de expresión*", que este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir información y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión. Entendiendo que la comunicación es un proceso social fundamental, una necesidad humana básica y el fundamento de toda organización social, que constituye, al fin y al cabo, el eje central de la Sociedad de la Información. Todas las personas, en todas partes, deben tener la oportunidad de participar, y nadie debería quedar excluido de los beneficios que ofrece la Sociedad de la Información.[29]

En este contexto, se introduce la inevitable necesidad de hacer referencia a Internet, como red de redes que ha venido a plantear un cambio al paradigma clásico del intercambio de información. Es precisamente a través de Internet que muchos de estos derechos previamente citados pueden llevarse a la práctica, efectivizarse, y es también esta nueva puerta de posibilidades quienes vienen a plantear obstáculos para el derecho, algunos que desarrollaremos a continuación.

1.7. Las Tecnologías de la Información y Comunicación y el Derecho

Bien conocidos son todos los beneficios o virtudes que ha traído consigo esta nueva era de la información. Desde la inmediatez o velocidad de las comunicaciones, la masividad en el procesamiento de datos, el acortamiento de las distancias, el acceso a la información, entre otras.

Sin embargo, no tantas veces se repara en el desarrollo de las problemáticas inherentes a su propio paradigma de la información, al menos, para el mundo jurídico. Por ejemplo, este "*desdibujamiento digital*" de las barreras clásicas, es

[29] CUMBRE MUNDIAL DE LA SOCIEDAD DE LA INFORMACIÓN; WSIS-03/GENEVA/4-S; 12 de mayo de 2004; Url: http://www.itu.int/wsis/docs/geneva/official/dop-es.html, Consultado: : 10 de Abril de 2014

reconocido por la Resolución AG/RES. 2004[30] que plantea la Estrategia de Seguridad Cibernética por parte de la Organización de los Estados Americanos (OEA), en donde se expresa que "*La naturaleza sin fronteras de las redes mundiales significa que un único acto delictivo relacionado con una computadora puede afectar o dirigirse a computadoras en varios países*".

Observamos entonces un primer desafío es presentado a través de la posibilidad de comunicación electrónica instantánea desde cualquier lugar del mundo, que implica como consecuencia directa el desvanecimiento de fronteras políticas tradicionales, una idea que hubiese espantado a muchos en otros tiempos.

Este fenómeno de la internacionalización en las comunicaciones, sin ningún tipo de "control" –un derecho humano garantizado como hemos visto- deja abierta la posibilidad de existencia de distintos tipos de acciones realizadas a través de los medios informáticos que pueden lesionar una variedad de derechos, que, al ser ejecutados desde cualquier lugar del mundo, posibilita el incremento de forma radical de sujetos activos por un lado, y pasivos por el otro. Dentro de esa puerta podemos encontrar una variedad de delitos como injurias, calumnias, amenazas, difamaciones, hackeos, interceptación de comunicaciones, extorsiones, entre otras. Delitos que, dicho sea de paso, adicionalmente a la posibilidad de ser cometidos a distancia a través de las nuevas tecnologías, estas conductas se ven facilitadas gracias a la posibilidad de la combinación de otros factores como el anonimato y la masividad.

La consecuencia fáctica de que dicha conducta desviada sea realizada de forma instantánea desde cualquier lugar del mundo implica que, para poder aplicar las consecuencias normativas correspondientes, será necesario determinar quién ha sido su autor, desde donde fue realizada dicha acción -con el problema que esto implica para la definición de la competencia-, conllevando así una compleja (y costosa en términos jurídicos y económicos) tarea de investigación. En el peor de los casos, dicha tarea puede incluso llegar a un camino sin salida, es decir, que sea imposible técnicamente determinar quién ha sido el autor de dicha acción. Es momento aquí entonces de identificar el segundo de los desafíos: el anonimato.

[30] ORGANIZACIÓN DE ESTADOS AMERICANOS (OEA); AG/RES. 2004 (XXXIV-O/04), Año 2004

La posibilidad de anonimato está al alcance de todas aquellas personas que con un mínimo conocimiento técnico, pueden utilizar determinadas herramientas técnicas para evitar ser rastreados (o que los rastros se pierdan en el medio de un océano), desarticulando las posibilidades de investigación (al menos de las clásicas) del derecho, quien rápidamente pierde fuerzas para hacer efectivo lo normado.

Este contexto, debe ser completado por el tercer y último elemento que desarrollaremos: la masividad. Este aspecto también viene a jugar un rol destacado en cuanto a los desafíos para el derecho, ya que, si bien la posibilidad de realizar una conducta dañosa siempre existió, las nuevas tecnologías posibilitan que dichas acciones se realicen de forma automatizada, permitiendo así la posibilidad de su comisión de forma masiva, al menos de una forma que nunca antes había sucedido. Tratando de trazar un paralelo (que desde ya advertimos que en el mundo digital, nunca son buenas las analogías), podríamos citar el ejemplo de un ladrón de casas, que una a una va probando las puertas de las casas, esperando encontrar alguna abierta en la oscuridad de la noche. En esta nueva versión digital del robo de información, un *cracker*[31] hoy se encuentra con la posibilidad de testear miles "de puertas informáticas", de forma simultánea y sin muchas complejidades técnicas. Es decir, esta masividad posibilita expandir el ataque de una forma nunca antes vista, multiplicando la cantidad de sujetos pasivos que recibirán el ataque, y multiplicando en consecuencia, las posibilidades de éxito del mismo.

Un claro ejemplo que permite confirmar esta última afirmación, son los engaños o estafas electrónicas, que son enviadas a diario a millones de correos electrónicos, esperando encontrar víctimas que caigan en las redes. Si bien del análisis de algunas de estas estafas parecen ser muy obvias en cuanto a su falsedad, como por ejemplo en el caso de la famosa "estafa nigeriana[32]", en general se estima que entre el 1 y 2% de los receptores de estas estafas, suelen ser exitosos. Si bien en principio la tasa de éxito parece baja, la posibilidad de enviar miles o millones de mensajes

[31] El término cracker (del inglés cracker, 'romper') se utiliza para referirse a las personas que rompen algún sistema de seguridad

[32] Esta estafa consiste en ilusionar a la víctima con una fortuna inexistente y persuadir para que pague una suma de dinero por adelantado, como condición para acceder a la supuesta fortuna. Las sumas solicitadas son bastante elevadas, pero insignificantes comparadas con la fortuna que las víctimas esperan recibir.

electrónicos de forma instantánea logra que dichas estafas aún resulten redituables para los ciberdelincuentes.

Otro bien jurídico clásico afectado con la posibilidad de difusión masiva, puede ser lo que sucede al publicar una foto privada en Internet (portales web o a través de canales de mensajería instantánea), como suele suceder en los conocidos casos del mal llamado "pornovenganza"[33]. Esto implica que dichos contenidos privados, son difundidos en forma masiva, haciendo que en la práctica sea técnicamente imposible determinar que otros terceros han visto, descargado y se encuentran en posesión de los contenidos indebidamente divulgados. Sostenemos que es inadecuada la denominación de pornovenganza, toda vez que el contenido pueda ser pornográfico, es necesario siempre contar con la voluntariedad de quienes participan en dichas representaciones, ya sea de forma amateur o profesional. En cambio, en muchos casos de este tipo, son contenidos obtenidos sin consentimiento.

1.8. La Eficacia del Derecho en la Sociedad de la Información

Superada la etapa teórica sobre algunos de los posibles conceptos sobre la eficacia del Derecho, y desarrollado algunos de los desafíos que la Sociedad de la Información vienen a plantear al mundo jurídico, estamos en condiciones de avanzar hacia el próximo paso.

Nuestro primer objeto inicial gira entonces sobre la posibilidad de análisis o reflexión de la siguiente pregunta: **¿Se ha visto afectada la eficacia del derecho en la Sociedad de la Información?**.

Siguiendo la doctrina autorizada en la materia, hemos ya dicho que la investigación para determinar la eficacia o ineficacia de una norma es de carácter histórico-social, de forma que se plantea el interrogante sobre si el cambio de las

[33] INFOBAE; "Crecen los casos de sextorsión y pornovenganza en el país: un hombre irá a juicio por viralizar videos íntimos de su ex"; Url: https://www.infobae.com/sociedad/policiales/2019/03/05/crecen-los-casos-de-sextorsion-y-pornovenganza-en-el-pais-un-hombre-ira-a-juicio-por-viralizar-videos-intimos-de-su-ex/

variables sociales ocasionadas por esta nueva Sociedad de la Información, han sido de tal naturaleza que tengan un impacto significativo sobre la eficacia del derecho actual.

A fin de construir las bases para sostener un ensayo de respuesta, se considera apropiado desarrollar brevemente algunas situaciones particulares sobre el derecho en relación con las nuevas tecnologías, útiles para ejemplificar la óptica o "lente" desde el cuál observamos al derecho.

1.9. El caso de la combinación entre Tecnología y Propiedad Intelectual

Dicho caso puede ser perfectamente aplicable en cualquier país del mundo, pero nos detendremos a repasar la situación actual en Argentina. En nuestro país se encuentra vigente la Ley 11.723, conocida como la Ley de Derechos de Autor, en la cual se establecen los criterios jurídicos esenciales del sistema de propiedad intelectual (siguiendo la línea internacional del Convenio de Berna).

Dicha norma, ha tipificado penalmente algunas conductas relacionadas a la violación de la propiedad intelectual, en los art. 71, 72 y 72 bis[34]. A modo general, dicha norma establece las reglas jurídicas sobre el régimen de propiedad intelectual, y no sólo eso, sino que, además, con el claro destino de reforzar su cumplimiento a través de la coacción, se ha optado por la utilización del instrumento más poderoso de todos (el penal), estableciendo distintas sanciones de prisión y multa para sus transgresores.

En palabras de una especialista en la materia, Beatriz Busaniche[35], "*Usuarios de Internet, bibliotecarios, docentes, estudiantes, consumidores, todo el mundo viola esta ley porque no hay forma de no hacerlo: Argentina no tiene excepciones*

[34] Ley 11.723; Art. 72 bis. — Será reprimido con prisión de un mes a seis años: a) El con fin de lucro reproduzca un fonograma sin autorización por escrito de su productor o del licenciado del productor;

[35] BUSANICHE, Beatriz; "El delito que cometemos todos", Fundación Via Libre. 2011. Url: http://www.vialibre.org.ar/2011/05/15/el-delito-que-cometemos-todos/

educativas, excepciones para bibliotecas, derecho a la copia privada, cláusulas de uso justo, o siquiera un derecho a cita lo suficientemente amplio para ser útil".

Más allá de la clara desactualización normativa en este ámbito (recordar que el texto de dicha norma data del año 1933), se debe reconocer que la posibilidad que se brinda a través de las nuevas tecnologías, donde ya no existe un "original" y una "copia", lo cual exige repensar todo o al menos, una gran parte del modelo de protección de la propiedad intelectual, el cual sigue representando actualmente para el derecho un claro desafío incluso a nivel mundial.

Es precisamente a este último punto al cuál queremos hacer referencia para apoyar la posición de este trabajo, es decir, las características inherentes a la Sociedad de la Información, han impactado en el modelo tradicional (en este ejemplo, de la propiedad intelectual) en algunos casos de una forma tan radical, que la versión "digital" de estos derechos (en el cuál, se aplica el mismo marco normativo) carecen de toda aplicación en los hechos, incluso existiendo sanción penal para dichas infracciones. Teniendo en consideración los distintos niveles de eficacia desarrollados de acuerdo a la teoría de Bobbio, en materia de propiedad intelectual, podríamos afirmar que estamos en presencia de la última de las opciones, con el nivel de eficacia más bajo.

1.10. El caso de la combinación entre Tecnología y Delincuencia

Entre los aspectos negativos que han venido de la mano las nuevas tecnologías, son probablemente los delitos informáticos los más importantes que se pueden encontrar, y es precisamente esta consideración la que en parte ha llevado a elegir a este tema como el núcleo central de esta tesis de doctorado.

De acuerdo a uno de los estudios más difundidos a nivel mundial en delitos informáticos[36], en el que se han entrevistado más de 13.000 adultos en 24 países,

[36] SYMANTEC CORPORATION; *Informe de Norton sobre delitos informáticos* para el año *2012*, septiembre de 2012: http://www.norton.com/2012cybercrimereport

para el año 2012, se calculó que los costos directos asociados con los delitos informáticos que afectan a los consumidores en el mundo ascendieron a US$ 110.000 billones en doce meses. El mismo estudio revela que por cada segundo 18 adultos son víctimas de un delito informático, lo que da como resultado más de un millón y medio de víctimas de delitos informáticos cada día, a nivel mundial.

Casos como los cables diplomáticos y secretos difundidos por Wikileaks[37], la aparición en la escena mundial de personas como Edward Snowden[38] y la apertura al mundo del programa de espionaje PRISM por parte de Estados Unidos, junto con otros tantos casos, van mostrando a la sociedad, la existencia de un entramado de información (confidencial o no) cada vez más importante, que en combinación con, traen consigo consecuencias sociales cada vez más grandes.

Presentado brevemente el entorno de esta problemática y sin ánimo de avanzar más para esta etapa del trabajo, estamos en condiciones de afirmar que la complejidad que reviste para el derecho puede analizarse desde distintos aspectos. Uno de esos aspectos, quizás el más importante desde el punto de vista jurídico, es precisamente la de contar con una legislación adecuada que permita condenar las conductas de ciberdelincuencia que sean consideradas como socialmente disvaliosas.

1.11. Los delitos informáticos como un desafío para el Derecho

Siguiendo la doctrina clásica y sin pretender abordar el tema con la profundidad que se merece y que más adelante veremos en detalle, podemos mencionar brevemente dos categorías de delitos informáticos: Por un lado, la comisión de

[37] DIARIO CLARIN, "La Casa Blanca implora a WikiLeaks que no filtre más documentos sobre la guerra", 30/07/2010. Url: http://www.clarin.com/mundo/Casa-Blanca-implora-WikiLeaks-documentos_0_307769448.html, Consultado: 27 de Noviembre de 2021

[38] DIARIO CLARÍN, "Hackeamos a cualquiera en cualquier parte del mundo". 11/06/2013. Url: http://www.clarin.com/mundo/Hackeamos-cualquier-parte-mundo_0_935906490.html, Consultado: 27 de Noviembre de 2021

delitos tradicionales a través de las nuevas tecnologías (por ejemplo, una estafa electrónica) y por otro, la existencia de nuevos bienes jurídicos tutelados (la información, la privacidad, etc.) que dan lugar a la existencia de nuevos delitos que hasta hace algunos años eran inexistentes, tales como el caso del *hacking, cracking,* etc.

En el ámbito penal material, en Argentina fue sancionada la Ley 26.388 (Junio de 2008), a través de la cual se ha incorporado diversos tipos penales relacionados a los delitos informáticos y que en el próximo capítulo analizaremos con mayor detalle.

En el ámbito procesal penal -ámbito que no será abordado en el presente trabajo, ya que por su importancia y complejidad, excedería el alcance de una tesis de doctorado-, aún existe una deuda en cuanto a la actualización de los códigos procesales penales argentinos, en los cuáles a criterio de este autor, debería darse una mayor importancia a la regulación sobre los procedimientos adecuados para la recolección y análisis de evidencia digital, aspectos prácticos imprescindibles para dotar de mayor eficacia lo normado materialmente.

Al desafío normativo, debemos sumar la posibilidad de comisión masiva e internacional de este tipo de delitos, originada en su posibilidad de realización a distancia y de forma instantánea, que termina potenciando aún más la realización de delitos, que forman un combo bastante complicado si se lo combina con la posibilidad de altos niveles de anonimato de algunas de las tecnologías disponibles.

Para no extendernos más en este punto, y a los fines de la introducción planteada en este capítulo, lo que se quiere señalar es que más allá de la existencia de una norma penal válida (en Argentina, la Ley 26.388 que ha incorporado la mayoría de estos tipos penales informáticos), la realidad del fenómeno demuestra un peligrosamente bajo nivel de eficacia.

1.12. La eficacia del Derecho en los Delitos Informáticos

Como hemos podido señalar en un principio, el objeto de este breve capítulo tenía como centro de gravedad invitar a la reflexión sobre si esta nueva Sociedad de

la Información -que ha llegado cargada en los hombros de los desarrollos tecnológicos de la información y las comunicaciones- ha generado o sigue generando cambios sociales de una entidad suficiente como para provocar ciertos cortocircuitos en el "orden social" tradicional, particularmente, afectando la efectividad del derecho vigente.

Teniendo ese interrogante como disparador y a criterio de este humilde autor, la respuesta -en determinados casos relacionados a las nuevas tecnologías-, es decididamente afirmativa, toda vez que algunos de los elementos característicos de esta nueva era, poseen un alto potencial que incide de forma directa en la eficacia de la norma.

Entre esos factores, observamos que los principales desafíos vienen dados por el elemento de la internacionalidad, masividad y anonimato -características propias de los delitos informáticos- generando una expansión radical sobre la cantidad y complejidad de conductas desviadas (en los términos de Durkheim). Este nuevo contexto, exige al derecho como sistema de control social, una mayor capacidad de respuesta ante las infracciones o bien, una reacción, una adaptación que permita corregir el rumbo que evite que muchas de esas conductas sigan navegando en una especie de mar en el cuál no llegan los brazos de la ley.

Esta nueva cantidad y complejidad de conductas desviadas realizadas a través de las denominadas nuevas tecnologías son las que, a criterio de este autor, afectan de forma significativa la efectividad del derecho, sobre todo en determinadas problemáticas puntuales como los delitos informáticos, tema central de esta tesis.

En otro orden de ideas, vale destacar que en los términos de los elementos del "control social" desarrollado en este trabajo, observamos que el desafío para el derecho por parte de las tecnologías de la información se encuentra más inclinado al aspecto formal que al material.

Es decir, en la deficiencia o ausencia de los mecanismos e instrumentos utilizados por parte del Estado para aplicar las sanciones dispuestas en el aspecto material. No queremos con ello disminuir la vital importancia del aspecto material, del cual se subyace la elemental necesidad de contar con una legislación actualizada y adaptada a los cambios y tiempos exigidos por esta Sociedad de la Información, y particularmente para el tema que nos ocupa: los delitos informáticos.

Por último, consideramos relevante dedicar unas breves líneas de estas reflexiones iniciales a expresar lo que llamamos como el efecto "sensación del vacío legislativo" en relación con la realización de conductas disvaliosas a través de las nuevas tecnologías. Este efecto -generado por una serie de condiciones que no serán analizadas en este trabajo- produce en la sociedad, un convencimiento acerca de que las reglas del derecho tradicionales no se aplican cuando las acciones se llevan a cabo en internet.

Desde el punto de vista técnico-jurídico, dicha sensación es en la mayoría de los casos infundada, toda vez que existe legislación aplicable -que, en su caso, podrá llegarse a debatir su idoneidad, pero que existe y está vigente-. De esta forma, la falta de información adecuada termina repercutiendo en el aumento de la cantidad de personas convencidas de que las conductas prohibidas en el mundo "físico", pueden ser realizadas en el mundo "virtual" de Internet sin recibir ningún tipo de correctivo o sanción por parte del sistema de derecho, perjudicando así aún más -en una especie de círculo vicioso- la situación de la eficacia del derecho.

A modo de reflexión de cierre este primer capítulo, que como ya hemos dicho, tiene por objeto hacer un primer acercamiento a la problemática observada por este autor, dejamos expresada la idea y la necesidad de evolucionar hacia un derecho más dinámico, menos cristalizado, que posea la potencialidad de dar respuestas más rápidas y justas ante una nueva gama de conductas desviadas que son apuntaladas por las características inherentes a la propia Sociedad de la Información.

Capítulo II: Delitos Informáticos y Cibercrimen.

2.1. Introducción

Al momento de la redacción de este trabajo, consideramos que ya no corresponde decir que estamos ante un nuevo fenómeno, o algo realmente nuevo. La realidad es que la delincuencia informática o ciberdelincuencia ya lleva varios años de gestación y desarrollo. En su caso, podríamos negociar aceptar la realización de una afirmación que lucirá como razonable para el/la lector/a: Si bien hace años que los delitos informáticos forman parte de la delincuencia en nuestra sociedad, no menos cierto es que en la última década el índice de ciberdelincuencia ha aumentado o al menos, es una problemática que a los ojos del ciudadano común, se puede visibilizar cada vez mejor. El paso del tiempo va generando los espacios necesarios para que el ciudadano vaya tomando conocimiento y dimensión de la existencia de este tipo de delitos.

En este aspecto, algunos casos mediáticos han sido útiles para dar a conocer los distintos riesgos que implican la utilización de las redes de información. Casos como el ciberataque mundial más grande que logró dejar sin sistemas a grandes multinacionales como Telefónica[39], junto con otros tantos casos nacionales[40] [41], van visibilizando cada vez más la existencia de una ciberdelincuencia creciente y cada vez más organizada.

[39] DIARIO CLARIN; "El masivo ciberataque ya afectó a 99 países e incluyó casi 150.000 incidentes", 12/05/2017. Url: https://www.clarin.com/mundo/masivo-ciberataque-afecto-74-paises-incluyo-45-000-incidentes_0_BJ9WEqXxb.html, Consultado: 20 de Mayo de 2021

[40] DIARIO LA NACIÓN; "También hackearon 30 correos del Ministerio de Seguridad". 01/02/2017. Url: http://www.lanacion.com.ar/1980702-tambien-hackearon-30-correos-del-ministerio-de-seguridad, Consultado: 20 de Mayo de 2021

[41] DIARIO CLARIN, "Denuncian que un hacker se robó $ 3.500.000 de una cuenta municipal". 23/11/2016. Url: https://www.clarin.com/policiales/denuncian-hacker-robo-cuenta-municipal_0_B1zeXn7Mx.html, Consultado: 20 de Mayo de 2021

Para comenzar con este capítulo, haremos un breve repaso sobre algunos conceptos básicos de la seguridad de la información, toda vez que estamos convencidos que para el objeto de esta tesis es necesario comprender algunos conceptos con claridad. Si bien no pretendemos adentrarnos demasiado en un desarrollo propio de sistemas, consideramos que dichos conocimientos son imprescindibles al momento de comprender los argumentos a partir de los cuáles giran los delitos informáticos.

Seguidamente introduciremos algunos conceptos tradicionales de la doctrina sobre delitos informáticos y cibercrimen, intentando desarrollar sus características generales y desafíos que representan para el derecho.

2.2. Aspectos básicos de la Seguridad de la Información

En gran parte, el aumento en la cantidad de incidentes de seguridad es razonable y desde el punto de vista de la seguridad de la información, hasta lógico que así ocurra. Intentaremos explicar este punto aprovechando que la formación de este autor, más allá del derecho, se vincula hacia la seguridad de las redes de información.

Según el Lic. Cristian Borghello[42], para comenzar el análisis de la Seguridad Informática se deberá conocer las características de lo que se pretende proteger: la Información. Así, definimos Dato como "la unidad mínima con la que se compone cierta información. "*Datum*" es una palabra latina, que significa "lo que se da"[43].

El citado autor sostiene que la Información "es una agregación de datos que tiene un significado específico más allá de cada uno de éstos", y tendrá un sentido particular según como y quien la procese. Ejemplo: 1, 9, 8 y 7 son datos; su agregación 1987 es Información.

[42] BORGHELLO, Cristian Fabian, Tesis "Seguridad Informática. Su Implicancia e Implementación"- 2001, Reg.UTN/Facultad 0015/793

[43] CALVO, Rafael Fernández. Glosario Básico Inglés–Español para usuarios de Internet. 1994–2000. Url: http://www.ati.es/novatica/2000/145, Consultado: 14 de Junio de 2022

En palabras del Lic. Cristian Borghello, “establecer el valor de la información es algo totalmente relativo, pues constituye un recurso que, en muchos casos, no se valora adecuadamente debido a su intangibilidad, cosa que no ocurre con los equipos, las aplicaciones y la documentación”.

Avanzando un paso más, diremos que todos los hechos no deseados donde se comprometa de cualquier forma la seguridad de la información, pueden ser considerado como un incidente de seguridad de la información. Tengamos en cuenta que estamos utilizando la palabra “información” y no “informática”, toda vez que esta disciplina (Seguridad de la Información), pretende abordar y trabajar por el aseguramiento de la información independientemente del medio en el cuál la misma sea almacenada o tratada -es decir, que aplica tanto para la información en bases de datos informatizadas, como para los ficheros en papel que tiene cualquier médico de la ciudad-.

Volviendo al punto anterior, todo incidente de seguridad puede ser estudiado -o debería-, a fin de determinar sus orígenes y en consecuencia poder trabajar sobre los diferentes riesgos que dieron lugar al mismo. La ciencia en esta disciplina está en su mayoría de acuerdo en afirmar que los riesgos pueden ser tener cuatro opciones: negados, reducidos, asumidos o transferidos. Entre ellas, lo que no debería suceder es negar la existencia de los riesgos, o al menos, es lo menos saludable para cualquier organización. La reducción o mitigación del riesgo es lo más normal o común de encontrar, que implica el trabajo sobre la implementación de diferentes medidas de seguridad que aportan a la disminución del riesgo -tengamos en cuenta, que nunca el riesgo podrá llevarse al mínimo, toda vez que no existe la seguridad absoluta-. Las otras opciones, implican por un lado asumir el riesgo, es decir que el responsable de la información sabe que existe el mismo y acepta someterse a la eventual ocurrencia de los incidentes de seguridad. Finalmente, la última opción es la transferencia del riesgo, que implica precisamente que un tercero pasa a asumir la responsabilidad para el caso de la ocurrencia del mismo -similar a lo que sucede con la contratación de cualquier póliza de seguros-.

Adentrándonos un poco más en el mundo de la seguridad de la información y aquí sí con mayor conexión hacia el tema madre de este trabajo, diremos que existen tres pilares básicos que se buscan o intentan resguardar: confidencialidad,

integridad y disponibilidad. Algunos autores agregan otros pilares, pero todos coinciden que estos tres, son los infaltables.

Recurriendo nuevamente a un especialista en Seguridad de la Información como el Lic. Cristian Borghello[44], citaremos sus definiciones sobre estos tres pilares:

La Integridad de la Información es la característica que hace que su contenido permanezca inalterado a menos que sea modificado por personal autorizado, y esta modificación sea registrada para posteriores controles o auditorías. Una falla de integridad puede estar dada por anomalías en el hardware, software, virus informáticos y/o modificación por personas que se infiltran en el sistema.

La Disponibilidad u Operatividad de la Información es su capacidad de estar siempre disponible para ser procesada por las personas autorizadas. Esto requiere que la misma se mantenga correctamente almacenada con el hardware y el software funcionando perfectamente y que se respeten los formatos para su recuperación en forma satisfactoria.

La Privacidad o Confidencialidad de la Información es la necesidad de que la misma sólo sea conocida por personas autorizadas. En casos de falta de confidencialidad, la Información puede provocar severos daños a su dueño (por ejemplo, conocer antecedentes médicos de una persona) o volverse obsoleta (por ejemplo: los planes de desarrollo de un producto que se “filtran” a una empresa competidora, facilitarán a esta última desarrollar un producto de características semejantes).

Dejamos aquí nuestro desarrollo en materia de seguridad de la información, prometiendo al lector recuperar estos conceptos y destacar la importancia de estos tres pilares, que en breve recuperaremos a fin de avanzar en nuestro estudio sobre los delitos informáticos.

[44] BORGHELLO, Cristian Fabian, Tesis "Seguridad Informática. Su Implicancia e Implementación"- 2001, Reg.UTN/Facultad 0015/793

2.3. La tecnología como potenciadora del delito

Cuando comenzamos este trabajo, adelantamos que ya no es posible afirmar que los delitos informáticos son algo novedoso, o un fenómeno al cuál deberíamos mostrarnos con sorpresa. Al menos no debería ser así para aquellos que se encuentran cercanos al mundo de la tecnología, o incluso, vinculados al ámbito del derecho penal.

A lo largo de la historia el delito en sí siempre ha encontrado en la tecnología un aliado, toda vez que los delincuentes siempre han utilizado las herramientas y tecnología a su alcance para lograr sus objetivos, incluso de formas bastante creativas.

No pretendemos aquí hacer un desarrollo exhaustivo del delito en sí, tarea que escapa al alcance de este trabajo, pero que, además, consideramos que para su mejor comprensión, debe recurrirse a la Criminología como ciencia que le propondrá al lector un abordaje mucho más amplio de lo que podríamos pretender realizar desde el derecho, y particularmente, desde el Derecho Penal.

A los fines de nuestro trabajo, y como operadores del derecho, no podemos dejar de considerar que será “delito” toda acción que así sea dispuesto por la ley. Desde nuestro punto de vista jurídico penal, entenderemos como delito toda acción típica, antijurídica y culpable, siguiendo la doctrina clásica[45] del Derecho Penal.

No obstante, y a los fines de advertencia para el lector, debemos confesar que en el tema de estudio, es muy común encontrar textos, artículos, libros y especialistas que se refieren a “delitos informáticos” y muchas veces se incluyen conductas que, al menos en Argentina, no se encuentran tipificadas penalmente.

Entiendo que dicha situación es consecuencia de varios factores, esencialmente de la existencia en el rubro de muchos profesionales de las ciencias informáticas, particularmente del ámbito de la seguridad de la información, cuyo concepto de delito no es estrictamente penal, y que la utilización de dicho concepto

[45] CREUS, Carlos, "Derecho Penal: Parte General", 5ta. Edición actualizada y ampliada. Editorial Astrea. 2010

en el marco de artículos y conferencias de seguridad de la información, generan confusiones.

Adicionalmente hay que mencionar la dificultad de abordar la temática desde una óptica nacional, ya que como hemos visto anteriormente, la problemática es de índole internacional o general, como todo fenómeno relacionado a las nuevas tecnologías, donde sus límites jurisdiccionales se tornan cada vez más borrosos. Realizada esta pequeña digresión, intentaré argumentar porque considero que las nuevas tecnologías son potenciadoras de los delitos.

Las nuevas tecnologías traen consigo muchísimos aspectos positivos a la vida de las personas, como la posibilidad de la comunicación instantánea, el contacto a distancia que incluso abre la puerta para miles de personas que pueden trabajar desde sus hogares, entre otra serie de grandes beneficios que no pretendemos aquí desarrollar.

Sin embargo, me concentraré en principio en solamente tres características de las tecnologías de la información y las comunicaciones: la inmediatez de las comunicaciones a distancia, la posibilidad de la realización de acciones masivas (automatizadas o no) y la posibilidad de realizar acciones con un determinado nivel de anonimato. Como habíamos adelantado también en el primer capítulo, estas tres características de las nuevas tecnologías son las que desde el punto de vista de este autor -y en combinación con una serie de factores que más adelante desarrollaremos- son la materia prima necesaria para generar el efecto potenciador de los delitos.

Muchos de los delitos clásicos -estafas, injurias, amenazas y hasta la propia distribución de pornografía infantil- existen desde mucho antes que existiera internet, y en algunos casos como las estafas, desde que el hombre se ha juntado en comunidad. Sin embargo, la combinación de la tecnología con muchos de estos delitos termina dando lugar a una nueva versión de los mismos, a un nuevo nivel en la comisión de estos mismos delitos. Y esta nueva etapa viene posibilitada de la mano de las características propias de las nuevas tecnologías que anteriormente citamos -inmediatez a distancia, masividad y anonimato-.

Por ejemplo, un estafador clásico, debía tomar sus recaudos en el tipo de engaño, acercarse a la víctima, tener habilidades sociales para ello, hacer incurrir en

el error a la víctima y con ello, lograr llevar adelante una estafa, siempre con el riesgo de ser descubierto, y que las personas hayan visto su cara.

Todos estos pasos vienen a ser casi automatizados en las estafas electrónicas, donde las posibilidades de éxito para el delincuente aumentan radicalmente. A través de herramientas tecnológicas, el delincuente podrá atacar múltiples víctimas a la vez (masividad), de forma instantánea (no se necesita esperar), llevando a cabo las maniobras desde cualquier lugar con conexión a internet (realización a distancia) y de acuerdo con el nivel de conocimiento del delincuente, hasta podrá utilizar determinados mecanismos que impidan su rastreo (anonimato).

De hecho, en el contexto de la Pandemia COVID-19, las estafas (sobre todo las bancarias) se incrementaron notoriamente, visibilizando que la imposibilidad o el hecho que por cuestiones gubernamentales la circulación se encontrará disminuida, una gran parte de la delincuencia decidió volcarse a la realización de estafas virtuales (ya sea a través del teléfono con posterior acceso indebido a las cuentas, o bien, todo a través de medios electrónicos).

Similar situación podríamos mencionar en el caso del delito de distribución de imágenes de abuso sexual infantil (mal llamado pornografía infantil), donde hasta hace algunos años, quienes detentaban este tipo de material debían revelar sus propias fotos, enviárselas a otras personas a través del correo postal, o hacer intercambios personales de los mismos. Actualmente, todo eso viene a facilitarse a través de las nuevas tecnologías, donde aquellos delincuentes que distribuyen o comercializan pornografía infantil, se encuentran cada vez con mayores posibilidades de continuar sus acciones delictivas.

Desde este punto de vista, opino que las tecnologías son potenciadoras de determinados tipos de delitos, que no son nuevos, que son clásicos, pero que al encontrarse en combinación con las características propias de las nuevas tecnologías de la información, terminan llevando al delito a un nuevo nivel de desarrollo, incrementando el daño realizado (caso de la distribución de la pornografía infantil), incrementando la cantidad de víctimas, dado que ya no importa en que barrio vive, el apellido, la ropa que lleva, o si lleva un arma de protección, sino que todos los usuarios conectados a internet se convierten en potenciales víctimas.

Por último, la utilización de herramientas de anonimización utilizadas por los delincuentes, en combinación con las dificultades propias para la determinación de la autoría en internet, terminan complejizando arduamente las tareas de investigación de los organismos competentes, que se ven compelidas a tener una actualización y capacitación constante para poder hacer frente a esta nueva gama de delitos.

Como cierre de este tema, y para evitar dejar un sabor negativo en la retina del lector, creo hacer necesaria la reflexión sobre la neutralidad de la tecnología en general, y de las nuevas tecnologías de la información y las comunicaciones (TICs) en particular.

No quisiera que la invitación o propuesta del razonamiento anterior, lleve al lector a pensar en la condena o estigmatización de las nuevas tecnologías, toda vez que considero como punto de partida filosófico que todas tecnologías son neutras. Es decir, que no son buenas ni malas en sí mismas, sino que ello dependerá de la intención de la persona que las utiliza.

No caben dudas que son incontables los beneficios que podríamos citar en la columna de los aspectos positivos, pero así también debemos hacernos cargo de que también posibilitan la realización de acciones negativas, entre ellos, una importante gama de delitos, tema que en definitiva, es objeto de esta tesis.

2.4. Delitos Informáticos. Conceptos y alcances

Para poder seguir avanzando en este trabajo, es necesario hacer aquí un punto de partida conceptual sobre el término “delito informático”, a fin de poder negociar con la persona lectora, un denominador común sobre su definición y sobre todo, su alcance.

Inicialmente debemos reconocer la inexistencia de un acuerdo en la doctrina acerca de su definición, así como la inexistencia de una norma (en Argentina) que ponga algún tipo de partida para aceptar o criticar jurídicamente.

De acuerdo con el histórico maestro Dr. Julio Tellez Valdes[46], estos delitos se pueden clasificar en sus formas típica y atípica, entendiendo por la primera a "las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin" y por las segundas "actitudes ilícitas en que se tienen a las computadoras como instrumento o fin". Si bien existen otros tantos conceptos en la doctrina, se toma el citado toda vez que su simple clasificación entre típicos y atípicos es útil a los fines de este trabajo. Aquí, solamente se consideran como "delito informático" a aquellos dentro de las categorías de los típicos, es decir, como una conducta penalmente sancionada por un país determinado.

La Organización para la Cooperación Económica y el Desarrollo (OCED) lo define como: "cualquier conducta, no ética, o no autorizada, que involucra el procesamiento automático de datos y/o la transmisión de datos".

Jijena Leiva los define como: "... toda acción típica, antijurídica y culpable, para cuya consumación se usa la tecnología computacional o se afecta a la información contenida en un sistema de tratamiento automatizado de la misma"[47]

En una subcategoría del propio concepto de delito informático, se plantea una decisión que, dependiendo de la postura adoptada, los delitos informáticos pueden ser un puñado de tipos penales, o bien, se multiplican de una forma considerable. Nos estamos refiriendo a que en algunos casos se decide utilizar el concepto de "delito informático" de forma reservado para aquellos tipos penales más específicos de la materia (por ejemplo, casos de hacking, cracking, denegación de servicios, grooming, etc.). Sin embargo, de acuerdo a una interpretación estrictamente jurídica del concepto ya desarrollado anteriormente, si la conducta típica se realiza a través de medios informáticos -a mi criterio esto es más correcto que decir que se realiza a través de "computadoras" como expone originalmente el Dr. Julio Tellez- también pasaría a ser un delito informático. ¿Es esto correcto? El autor Miguel Angel Davara Rodríguez[48] define el delito informático como "*la realización de una acción, que*

[46] TÉLLEZ VALDÉS, Julio, "Derecho Informático", 3ª.ed., Ed. Mc Graw Hill, México, 2003, Pág. 8

[47] JIJENA LEIVA, Renato Javier: "La Criminalidad Informática": Situación de Lege Data y Lege Ferenda en Chile". Actas de III Congreso Iberoamericano de Informática y Derecho". Mérida, España.

[48] DAVARA RODRIGUEZ, Miguel Ángel, Manual de Derecho Informático, Thomson Aranzadi, 10º edición, pág. 358 y 359.

reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software". Agregando luego: "*Nos estamos refiriendo solamente, a la comisión de un delito por medios informáticos o telemáticos, ya que la comisión de otros delitos en los que alguna forma interviene un elemento informático, se encontrará sin duda dentro del Derecho Penal General*".

Es decir, este autor parece darse cuenta de la importancia de definir cuál será el alcance que le daremos al concepto, y del riesgo que implicaría en su caso que cualquier participación menor de la tecnología en un delito, termina por "convertirlo" en un delito informático.

A mi criterio, la respuesta es positiva y negativa a la vez. Es decir, en principio debe dejarse en claro que la mera intervención de un elemento informático no convierte a un delito clásico en un delito informático. Sin embargo, es necesario reconocer que, en determinados tipos penales, el ingrediente tecnológico es tan poderoso -de acuerdo a lo explicado sobre la potencialidad- que hace necesario que para su identificación, investigación y persecución intervengan especialistas dedicados a los delitos informáticos.

Es decir, hablamos de aquellos casos donde el tipo penal clásico es perfeccionado utilizando a las nuevas tecnologías como medio para su comisión, dotándolo de esa manera de muchos de los inconvenientes o desafíos clásicos de los delitos informáticos, tales como el anonimato, internacionalidad, dificultad en la obtención de evidencia digital, entre otros.

Podría legítimamente el lector preguntarse cuál sería la diferencia de considerar que el delito sea considerado o no un delito informático, o si bien, se trata de una discusión meramente doctrinaria. En principio, la respuesta no parece ser tan importante toda vez que en Argentina y a modo de adelanto, este tipo de delitos no generan una nueva categoría penal que pudiera derivar en la aplicación o no de un régimen jurídico especial. No obstante, podría tornarse de interés a los fines de

definir la jurisdicción y la competencia, recordando que en nuestro país ya empiezan a surgir las primeras fiscalías especializadas en ciberdelincuencia[49].

2.5. Cibercrimen y ciberdelincuencia

No podemos continuar sin abordar las diferencias entre el concepto de cibercrimen y ciberdelincuencia, o bien, delitos informáticos y cibercrimen, conceptos que normalmente son utilizados como sinónimos pero que a fines académicos y doctrinarios tienen diferencias que nos parece aquí el momento adecuado para señalarlas.

Principalmente la diferencia radica en la organización del delito. Es decir, cuando nos referimos a delitos informáticos, delincuente informático o ciberdelincuencia, nos referimos a aquellos delitos que ocurren a diario, tipificados penalmente, pero que ocurren de forma independiente, o individual, sin coordinación propia u organización en sí.

Bastaría dar como ejemplo un caso de acceso indebido a una cuenta de correo electrónico, de una persona a su expareja. O bien, el empleado enojado que borra información importante (*inside job*) para la organización. Podríamos también mencionar (ya como delitos informáticos de segundo nivel), una amenaza de muerte realizada vía correo electrónico, o whatsapp. O las injurias o calumnias realizadas desde un perfil falso de Facebook.

El denominador común de todos los casos mencionados es que los delitos existen, ocurren, pero se cometen o llevan a cabo de forma aislada o independiente. Es decir, el autor delincuente, lo realiza por distintos motivos, pero no hace de ello una forma de vida.

En cambio, cuando nos referimos al cibercrimen, estamos hablando de una serie de delitos informáticos que, sí ocurren de una forma más profesional, organizada, sin motivaciones personales más que las económicas. Donde no

[49] Diario CLARIN, "Una fiscalía dedicada a los delitos informáticos", Url: https://www.clarin.com/policiales/fiscalia-dedicada-delitos-informaticos_0_rkQlLoiv7x.html, Consultada: 13 de Junio de 2017

importa quién es la víctima, porque son elementos fungibles y sin interés para la banda, que busca optimizar sus ganancias a través del perfeccionamiento de distintas técnicas delictivas que utilizan a la tecnología como eje.

Como ejemplo claro podemos mencionar los ataques de *ransomware*, un tipo de malware (software malintencionado) que tiene como objetivo bloquear el uso del ordenador o parte de la información que contiene, para después poder pedir un rescate a cambio de su liberación.

Estas bandas de ciberdelincuentes no están para nada interesados en el objetivo, en la víctima, en su información en sí, sino que el objetivo en atacar la disponibilidad de la información de la víctima, y por supuesto, cobrar un rescate para devolver la misma. Es un negocio organizado, con personas que se dedican a desarrollar el malware, otros a infectar sistemas, otros a la "atención al cliente" vía foros o correo electrónico, donde se indican cuánto y cómo se debe pagar el rescate. Hay líderes en las bandas, personas dedicadas a la gestión de las billeteras virtuales (que no duran más que unos días), otros al blanqueo del dinero, entre otras tareas.

Similar ejemplo, pero de quizás menos organización que estas nuevas bandas, pero que siguen siendo un clásico del cibercrimen, son las dedicadas a las estafas electrónicas. Aquí nuevamente podremos encontrar bandas con aquellos dedicados a la captación ilegítima de datos confidenciales -datos de las tarjetas de crédito por ejemplo-, generalmente a través de técnicas de *phishing*. El phishing es una técnica de ingeniería social utilizada por los delincuentes para obtener información confidencial como nombres de usuario, contraseñas y detalles de tarjetas de crédito haciéndose pasar por una comunicación confiable y legítima[50].

En estas bandas podemos encontrar a los diseñadores de las páginas mellizas, los que se encargan de la distribución vía spam, los que recolectan los datos, los procesan y en algunos casos los venden en el mercado negro, quienes compran esos datos (o es la misma banda que los utiliza), quien realiza las propias estafas (ardid o engaño y un perjuicio patrimonial), las mulas, blanqueadores, etc. Nuevamente, vemos aquí un grupo de personas que hacen de estos delitos un

[50] SEGU-INFO, "Phishing", Url: http://www.segu-info.com.ar/malware/phishing.htm

oficio, donde pueden verse notas de organización y realización de forma masiva, de forma continuada.

De acuerdo a un estudio realizado por una empresa de seguridad Panda Security[51], las mafias de ciberdelincuentes que operan en Internet están muy organizadas, tanto desde el punto de vista de visión estratégica como desde la operativa, logística y despliegue de sus operaciones. Y, además, no sólo pueden parecer verdaderas compañías, sino que son organizaciones multinacionales, ya que operan a lo largo y ancho del planeta.

De este último informe, se ha extraído una clasificación publicada por el FBI, de las diferentes "profesiones" del mundo de los cibercriminales, en un intento de tipificar las figuras más comunes que podemos encontrar en el proceso mafioso de generar dinero mediante el robo, la extorsión y el fraude a través de Internet.

Según el citado informe, el FBI considera que las organizaciones cibercriminales funcionan como empresas, contando con expertos especializados para cada tipo de trabajo y ocupación. A diferencia de una organización empresarial, estos cibercriminales trabajan sin horarios, sin vacaciones y sin fines de semana. Entre las especializaciones más comunes que tipifica el FBI son las siguientes:

***1. Programadores**. Desarrollan los exploits y el malware que se utiliza para cometer los cibercrímenes.*

***2. Distribuidores**. Recopilan y venden los datos robados, actuando como intermediarios.*

***3. Técnicos expertos.** Mantienen la infraestructura de la "compañía" criminal, incluyendo servidores, tecnologías*

de cifrado, bases de datos, etc.

***4. Hackers.** Buscan aplicaciones exploits y vulnerabilidades en sistemas y redes.*

***5. Defraudadores**. Crean técnicas de ingeniería social y despliegan diferentes ataques de phishing o spam, entre otros.*

***6. Proveedores de hosting.** Ofrecen un entorno seguro para alojar contenido ilícito en servidores y páginas.*

[51] PANDA SECURITY, "El mercado negro del Cibercrimen", 2010. Url: http://prensa.pandasecurity.com/wp-content/uploads/2011/01/Mercado-Negro-del-Cybercrimen.pdf, Consultado: 27 de Noviembre de 2013

7. Vendedores. *Controlan las cuentas y los nombres de las víctimas y las proveen a otros criminales mediante un pago.*

8. Muleros. *Realizan las transferencias bancarias entre cuentas de banco.*

9. Blanqueadores. *Se ocupan de blanquear los beneficios.*

10. Líderes de la organización*. Frecuentemente, personas normales sin conocimientos técnicos que crean el equipo y definen los objetivos.*

Según este estudio, las organizaciones cibercriminales se organizan de forma jerárquica, y cada paso diferente de la cadena cuenta no con uno, sino con varios especialistas.

Como puede observarse, existen distintos niveles o grados de profesionalización entre los delincuentes (como en muchos otros delitos) en materia de delitos informáticos. Por lo general, suele pensarse que los delincuentes informáticos actúan de forma aislada, espontánea, independiente, de acuerdo con distintas motivaciones. Sin embargo, el transcurso del tiempo y la experiencia en los delincuentes trae consigo la existencia de redes organizadas dedicadas a la comisión de delitos cada vez más complejos y la problemática está escalando en gravedad debido a la existencia de cada vez mayores redes internacionales dedicadas a este tipo de delitos.

Sobre estas bandas organizadas y relacionado con el delito de la comercialización de contenidos de abuso sexual infantil a través de medios informáticos, se pueden citar en Argentina distintos casos de desbaratamientos de complejas redes. En el año 2012 por ejemplo, a través de la denominada "Operación Oliver"[52], nacida bajo una investigación previa realizada en Londres, se realizaron 11 allanamientos en la ciudad de Buenos Aires, 24 en el conurbano bonaerense y 26 en distintas provincias (Salta, Tierra del Fuego, San Juan, Tucumán, Santa Fe, Santa Cruz, Córdoba, Santiago del Estero, Chaco, Entre Ríos y Neuquén), con la imputación de 64 personas involucradas.

[52] SECRETARÍA DE COMUNICACIÓN PÚBLICA DE LA PRESIDENCIA DE LA NACIÓN, "La Policía Federal desarticuló una red internacional de pornografía infantil". Url: http://www.prensa.argentina.ar/2013/01/11/37634-la-policia-federal-desarticulo-una-red-internacional-de-pornografia-infantil.php, Consultado: 27 de Noviembre de 2021

2.6. Hackers vs. Crackers

Dentro del campo de los delitos informáticos, la intromisión ilegal a los sistemas de información (junto a los ataques de denegación de servicios) han sido desde los comienzos, los delitos clásicos a combatir.

Es común escuchar o leer el concepto de hacking o hacker, asociado a la intrusión en sistemas informáticos, seguidos de robo de información, modificación de datos, hasta incluso, cuando existe supresión de la información. En la generalidad de las veces, esta mala utilización del vocablo, es empujado y alimentado por los medios masivos de comunicación que, por lo general, responden a dos factores de desconocimiento: interno y externo.

Interno, porque quienes están a cargo de la redacción de la noticia, desconocen el tema, y por lo tanto, ante un hecho que acontece, deciden encabezar el título utilizando ese vocablo al estilo de “Hackearon el Poder Judicial de Chaco” o “Hackearon el Senado de la Nación”, por citar algunos casos de la actualidad.

Externo, es por el propio desconocimiento social sobre el concepto hacker. Es decir, el común de las personas, sin conocimientos avanzados ni profundos en materia de informática, en su mente, al darle significado a tal vocablo, su representación es precisamente aquella que aprendieron de los propios medios de comunicación, ya sea a través de las propias noticias, películas o internet, haciendo que el aspecto interno y externo se retroalimentan, generando cada vez más degeneración del concepto.

Al momento de buscar la raíz, la fuente de más confianza es sin dudas acudir al Jargon File, un diccionario informático, construido por informáticos. En él se han recolectado los significados más utilizados dentro de la cultura técnica de los centros de desarrollo más grandes de informática (MIT, SAIL, CMU, WPI, entre otras)[53].

En una pequeña digresión, pero de importancia para comprender la fuente y la entidad del contenido en tal diccionario, diré que el Jargon File fue iniciado por

[53] Instituto Tecnológico de Massachusetts (MIT); Laboratorio de IA de Stanford (SAIL), Universidad de Carnegie-Mellon (CMU), Instituto Politécnico de Worcester (WPI).

Raphael Finkel en 1975, aunque incluso algunos términos datan de años anteriores. Al comienzo, el archivo estaba muy orientado a conceptos relativos a la Inteligencia Artificial, pero con el tiempo, se fue ampliando. Años después, Richard Stallman[54] realizó grandes aportes, en lo relativo a términos de MIT e ITS.

Dentro del Jargon File[55], podemos encontrar el concepto de hacker y cracker, con las diferentes acepciones consideradas, donde se han ido plasmando las diferentes acepciones que podemos llegar a conocer de este vocablo, algunas de ellas, más que interesante para profundizar.

Comenzamos destacando el concepto utilizado para “hacker”:

> ***hacker**: n.1. Originalmente, alguien que hace muebles con un hacha.*
>
> *1) Una persona que disfruta explorando los detalles de los sistemas programables y en cómo extender sus capacidades, a diferencia de la mayoría de los usuarios, que prefieren aprender sólo el mínimo necesario. En RFC1392, un glosario de los usuarios de Internet, ayuda ampliándolo como: Una persona que se complace en tener un conocimiento íntimo del funcionamiento interno de un sistema, las computadoras y redes informáticas, en particular.*
>
> *2) Alguien que programa con entusiasmo (incluso obsesivamente) o que disfruta de la programación y no sólo teorizar acerca de la programación.*
>
> *3) Una persona capaz de apreciar el “valor hacker”.*
>
> *4) Una persona que es buena programando rápido.*
>
> *5) Un experto en un programa en particular, o uno que con frecuencia no funciona, como en "un hacker de UNIX". (Definiciones de 1 a 5 están correlacionadas, y las personas que se ajustan a ellas se congregan.)*
>
> *6) Un experto o entusiasta de cualquier tipo. Uno puede ser un hacker de la astronomía, por ejemplo.*
>
> *7) Uno que disfruta el reto intelectual de superar o sortear creativamente las limitaciones.*
>
> *8) (obsoleto) Un entrometido malicioso que intenta descubrir información sensible por curiosidad. Por ejemplo: hacker de contraseñas, hacker de la red. El término correcto para este sentido es cracker.*

[54] Richard M. Stallman, Programador Estadounidense, Fundador del Movimiento de Software Libre, la FSF y el Proyecto GNU.

[55] JARGON FILE; Versión 4.4.7, modificada por última vez el 29 de Diciembre . www.catb.org/jargon

> *El término hacker 'también tiende a connotar pertenencia a la comunidad global definida por la red (consulte la red. Para la discusión de algunos de los fundamentos de esta cultura, consulte el Cómo hacer en el FAQ Hacker). También implica que la persona descrita se considera suscripta a alguna versión de la ética hacker (véase la ética hacker). Es mejor ser descrito como un hacker por otros que para describir a sí mismo de esa manera. Los hackers se consideran algo de una élite (una meritocracia basada en la capacidad), aunque se reciben a los nuevos miembros de buen grado. Así pues, es la satisfacción del ego que se había determinado en la identificación de sí mismo como un hacker (pero si una persona se jactase de ser un hacker y no lo es, rápidamente se los etiquetará como un fraude). Véase también geek, wannabee. Este término parece haber sido adoptado por primera vez como una insignia en la década de 1960 por la cultura hacker que rodean TMRC y el Laboratorio de Inteligencia Artificial del MIT. Tenemos un informe que se utilizó al concepto en un sentido restringido por radioaficionados adolescentes y experimentadores electrónicos, a mediados de la década de 1950.*

Tal como se señala en final del punto 5, las primeras cinco acepciones, giran alrededor de un marco de características comunes, resumiéndolas como "*una persona experta en programación, que conoce íntimamente los sistemas y la red, que disfruta explorando sus límites, descubriendo desafíos y comprendiéndolos, cuyo fin es experimentar diferentes alternativas para vencer el sistema, sin tener intereses en la información que exista dentro del mismo (valor hacker)*".

Este primer concepto de hacker, al cuál en este trabajo me referiré como de carácter restringido, dado que, si bien conserva los caracteres comunes de la actividad, la misma es siempre circunscripta al contexto de la informática, los ordenadores, sus sistemas y las redes. Con este sentido, utilizaré el concepto de hacker a lo largo de este trabajo.

En el punto 3 del concepto de hacker del Jargon File, introduce un elemento que a nuestro criterio es de suma importancia: el "valor hacker", dando un vínculo hacia la concepción del mismo glosario informático.

> ***"Hack value";*** *Generalmente presentado como la razón o motivación para el esfuerzo con un objetivo aparentemente inútil, donde el punto es que la meta lograda es una de poca entidad [...]. Por ejemplo, MacLISP tenía características para leer e imprimir los números romanos, que fueron instalados exclusivamente para lograr este valor hacker. Mirar una*

pantalla de hack es un método de cálculo del valor hack, pero esta realidad no se puede explicar, sólo a través de la experiencia. Como Louis Armstrong dijo en una ocasión cuando se le pide que explique de jazz: "Hombre, si tienes que pedir que te lo expliquen, es que nunca lo has conocido. Url: http://www.catb.org/jargon/html/H/hack-value.html

Consideramos de importancia la significación del valor hacker, ya que expresa el aspecto subjetivo más genuino del hacking puro o de sombrero blanco, que luego deberemos tener en cuenta al analizar el tipo penal. En relación a lo que veníamos desarrollando anteriormente con respecto a la finalidad, este valor hacker expresa la idea que la persona que lleva adelante esa acción no se interesa en el final -meta lograda u objetivo, que sería el acceso a la información del sistema- sino que su foco se concentra en el método utilizado para lograrlo -proceso para sortear los límites del sistema-.

Queda claro entonces que la marca distintiva del valor hacker es el reto intelectual, necesitando en consecuencia dos factores. Primero una persona con verdadero y profundo conocimiento sobre alguna materia. Segundo, la existencia de desafíos técnicos que supongan alguna dificultad para la persona, que incentive a resolver el enigma, a utilizar su conocimiento como base y su mente creativa como herramienta para generar distintas formas de saltarse dichas limitaciones.

Encontramos este concepto en el autor Pekka Himanen, en su obra más difundida desarrolla los fundamentos y consecuencias de la ética hacker[56]. En el prólogo de dicho libro, Linus Torvalds[57], desarrolla de manera impecable una explicación sobre el tema del valor hacker, al hablar sobre el tema de las motivaciones. A través de su “ley de Linus”, categoriza las motivaciones en 3 escalones: supervivencia, vida social y entretenimiento (en mayúscula).

Linus Torvalds sostiene que el entretenimiento es aquello que está más allá de la supervivencia y la vida social. Es cualquier ejercicio mental del individuo, que tenga como fin explicar para sí el universo. Da un ejemplo nombrando a Einstein, afirmando que él no estaba motivado por la supervivencia cuando pensaba en la

[56] HIMMANEN, Pekka. “La ética hacker y el espíritu en la era de la información”. Edición Digital de Licencia GPL. Url: http://www.educacionenvalores.org/IMG/pdf/pekka.pdf

[57] LINUS, Torvalds. Creador del Sistema Operativo Linux y uno de los hackers más respetados de la comunidad.

física, ni por cuestiones sociales, sino por algo que excede todo aquello, que era su pasión, su motivo, su ENTRETENIMIENTO (con mayúsculas). Termina definiéndolo como algo intrínsecamente interesante y capaz de plantear desafíos.

A modo de cierre de este repaso terminológico, abordaremos la conceptualización dada en el Jargon File sobre la figura del *cracker,* donde advertimos con mayor claridad las diferencias entre una actividad y otra, que tiene tanta relevancia a nivel objetivo como subjetivo.

> ***cracker**; Aquel que rompe la seguridad en un sistema. Acuñado en 1985 por hackers en defensa contra el mal uso periodístico del hacker (ver el sentido 8). Si bien se espera que cualquier verdadero hacker habrá hecho algún juego de grietas y conoce muchas de las técnicas básicas, cualquiera que haya pasado esa etapa de larva, se espera que ya no caigan en el deseo de hacerlo, a excepción que se necesite inmediatamente, de manera benigna y por razones prácticas (por ejemplo, si se trata de resolver algunos de seguridad con el fin de trabajar un poco). Por lo tanto, hay mucho menos de solapamiento entre los hackers y crackers que el lector mundano cree, engañado por el periodismo sensacionalista. Los crackers tienden a reunirse en pequeños, muy unidos. A menudo les gusta describirse a sí mismos como hackers, piratas informáticos, cuando estos los consideran una forma separada e inferior de vida. Url: http://www.catb.org/jargon/html/C/cracker.html*

Como podemos observar, la conceptualización es radicalmente distinta, que claramente denota la frustración que existe por las confusiones mediáticas entre hackers y crackers. Tratando de realizar un abordaje comparativo entre los mismos, entendemos que el cracker al comprobar la vulnerabilidad existente, buscará la manera de explotarla para acceder al sistema, pero totalmente enfocado en la existencia de información valiosa en su interior, normalmente copiando, modificando o suprimiendo la misma. En la mayoría de los casos, modifican o agregan información, con leyendas que hagan referencia a su paso por el sistema, con la finalidad de alimentar su ego y poder mostrarlo a sus pares (meritocracia degenerada), como aquel ladrón que antes de irse pinta la pared con algún mensaje alusivo.

A nivel comparativo podríamos señalar que los hackers, al testear y comprobar vulnerabilidades de seguridad, por sus propios principios, no dañan (sentido general

de no copia, no modificación, no supresión, etc.) la información contenida, siendo que, en muchos casos, ni siquiera existe un real acceso a la información sino a su contenedor, el sistema en sí. El hacker, al retirarse del sistema, se encarga de buscar la forma de hacer saber a quién tiene el sistema a cargo (administrador por lo general), la existencia de vulnerabilidades. En algunas ocasiones, dependiendo del caso y la complejidad del problema, se realizan sugerencias sobre posibles soluciones para mitigar dicha vulnerabilidad.

Estas diferencias son también claras a nivel subjetivo, donde el hacker tiene intenciones de mejorar sus habilidades en la programación y la comprensión de los sistemas, donde el incentivo es un desafío intelectual y no la violación de secretos ni privacidad alguna. Por ello es por lo que el foco está puesto en los sistemas en sí, y no en la información que contienen.

En el cracker, la finalidad perseguida sí es la información resguardada detrás de alguna barrera, la vulneración de secretos. Muestra clara de ello, es la irrelevancia sobre el "cómo se accede" a la misma, que puede ser con técnicas básicas o incluso utilizando algún rootkit[58] automatizado, denotando lo inverso al hacker. El foco no es el sistema, sino lo que se esconde detrás, la información. Este germen del cambio de objetivo, es lo que a lo largo del tiempo viene a dar lugar a la generación de las bandas organizadas de cibercrimen, que como hemos ya dicho en puntos anteriores, se profesionalizan en automatizar ataques buscando obtener el mayor rédito posible en la menor cantidad de tiempo.

2.7. Hacking: categorías y posturas doctrinarias

Tomando la clasificación realizada por el Dr. Claudio Manzur[59], se señala que el hacking puede clasificarse en directo o indirecto. Será directo (también conocido

[58] Un rootkit es una herramienta, o un grupo de ellas que tiene como finalidad esconderse a sí misma y esconder otros programas, procesos, archivos, directorios, claves de registro, y puertos que permiten al intruso mantener el acceso a un sistema para remotamente comandar acciones o extraer información sensible.

[59] MANZUR, Claudio Líbano. "Chile: Los Delitos de Hacking en sus Diversas Manifestaciones", (Revista Electrónica de Derecho Informático). Abogado Profesor. Director Secretario Ejecutivo de la Asociación de Derecho e Informática de Chile (ADI-CHILE)

como mero intrusismo) el hacking propiamente dicho, explica este autor, que consiste en acceder de manera indebida, sin autorización o contra derecho a un sistema de tratamiento de la información, con el fin de obtener una satisfacción de carácter intelectual por el desciframiento de los códigos de acceso o passwords, no causando daños inmediatos y tangibles en la víctima, o bien por la mera voluntad de curiosear o divertirse de su autor.

La voluntad de divertirse generalmente se traduce en paseos por el sistema haciendo alarde de la intromisión. Es por ello que esta delincuencia se ha nominado "short pants crimes", es decir, crímenes en pantalones cortos; su motivación no es la de causar un daño, sino que se trata de obtener personales satisfacciones y orgullos, basados principalmente en la burla de los sistemas de seguridad dispuestos. Esta clase de hacking no representa un importante nivel de riesgo, toda vez que el hacker no busca causar un daño.

En lo que atañe al hacking indirecto, este autor considera que es el medio para la comisión de otros delitos como fraude, sabotaje, piratería, y espionaje. Señala que, en el caso del hacking indirecto, el ánimo del delincuente está determinado por su intención de dañar, de defraudar, de espiar, etc., entendiendo que no desaparece el delito de acceso indebido, dándose la hipótesis del concurso ideal o formal de los delitos.

El Dr. Hugo Carrión[60], realiza algunas consideraciones muy interesantes sobre la clasificación del Dr. Manzur. Sostiene que, si el acceso ilegítimo al sistema informático es el medio para alterar, modificar o suprimir la información, no habrá hacking sino cracking que supone una acción concreta de daño sobre la información y el elemento subjetivo en el autor –dolo- constitutivo del conocimiento y la voluntad de provocarlo.

En lo que respecta a las figuras de hacking y cracking, discrepa en que se verifique el supuesto de concurso ideal de delitos. Como señala, el hacking es el presupuesto necesario del cracking (todo crack supone un hack previo), pero cuando

[60] CARRION, Hugo Daniel. "Presupuestos para la punibilidad del hacking", *1° Jornadas Latinoamericanas de Derecho Informático, Organizacón Mundial de Derecho e Informática,* Mar del Plata, 2001. [http://www.delitosinformaticos.com/trabajos/hacking.pdf]

se consuma este ilícito, el anterior queda subsumido en él por reunir las exigencias del tipo, dándose un concurso aparente de delitos por razones de especialidad. Lo contrario importa una doble persecución penal (non bis in idem), situación que se encuentra proscrita por el principio constitucional de legalidad.

Para una especie diferente del hacking, como lo es el hacking ético, siendo este una actividad desarrollada por profesionales de la seguridad como servicio para empresas u organizaciones que quieran informarse acerca del estado de seguridad de sus sistemas. De esta manera, previo permiso y consentimiento del titular de los sistemas, el profesional habilitado utiliza diferentes técnicas de ataque, tal como utilizaría algún sujeto extraño que quisiera colarse por esos sistemas vulnerando la seguridad, a fin de confeccionar un informe. Este tipo de actividad, como ya veremos desde el punto de vista de la normativa argentina, es plenamente lícita, ya que queda fuera del tipo penal al considerarse que en estos casos, no se da el requisito de "indebido" (dada la expresión de consentimiento del titular) que exige el tipo penal de Argentina.

Desde hace tiempo existe la discusión sobre la intervención del derecho penal sobre el hacking#, no sólo en nuestro país sino a nivel general. En Agosto de 2021, entre las organizaciones Access Now y Fundación Vía Libre, generaron un importante documento denominado "Persecución de la comunidad de infosec en América Latina", donde precisamente se aborda la existencia de casos paradigmáticos en Argentina, Colombia, Ecuador y México. En los capítulos finales abordaremos nuevamente esta temática.

Volviendo al desarrollo doctrinario, en una primera etapa la discusión giró alrededor de si debía o no punirse el hacking. Una primera posición encuentra a aquellos que no consideran que el hacking sea una conducta disvaliosa de tal entidad que justifique la participación del derecho penal (pero que sí podría traer consecuencias de responsabilidad civil).

Personalmente adhiero a la opinión del Dr. Marcelo Riquert, quien al comentar la redacción del art. 153 bis incorporado al Código Penal Argentino, expresa su diferencia en el tema: "*Entendemos que habiéndose optado por la criminalización de esta conducta disvaliosa resignando la vía contravencional, al menos podría haberse*

evitado la utilización de la pena privativa de libertad en la figura básica. Es claro que no sólo en el imaginario colectivo, sino en la mente del legislador, sigue instalada férreamente la idea de que "penar" significa "privar de libertad". No albergo dudas de que estamos frente a una conducta que tendría una respuesta punitiva más racional si se la hubiese conminado con multa o alguna inhabilitación especial o alternativa reparatoria."

Posición similar fue considerada y fundamentada en el anteproyecto del 2001, coordinado por la Dra. Mercedez Vazquez, que si bien considerada la actividad como ilícito penal, afirma: "*Consideramos apropiada aquí, la fijación de una pena de multa, atento que se trata de una figura básica que generalmente opera como antesala de conductas más graves, por lo que no amerita pena privativa de la libertad, la que por la naturaleza del injusto habría de ser de muy corta duración. Este criterio resulta acorde con el de las legislaciones penales más modernas (Alemana, Austríaca, Italiana, Francesa y Española), que ven en la pena de multa el gran sustituto de las penas corporales de corta duración, puesto que no menoscaban bienes personalísimos como la libertad, ni arrancan al individuo de su entorno familiar y social o lo excluyen de su trabajo.*"

En el otro extremo, se encuentra la posición que exige considerar al hacking como conducta delictiva, como delito de peligro, teniendo en consideración las supuestas implicancias negativas que existirían socialmente si el legislador penal no tomará intervención en el asunto.

No habría dudas en el caso del cracking, donde existe un daño real y concreto sobre la información, justificando así la sanción penal.

Dentro de esta última posición, que es sin duda la receptada por la mayoría de los países (y la receptada por el Convenio de Cibercrimen de Budapest que más adelante analizaremos), podemos distinguir una nueva dicotomía, presentando por un lado a aquellos que adhieren a una posición de castigar la actividad del hacking directo (o mero intrusismo) con pena privativa de la libertad, frente a aquellos que consideran que es suficiente con una sanción de multa y/o inhabilitación, dejando la pena de prisión para el caso de la producción real de un daño o apropiación de datos en un sistema informático (crack).

Aquellos que consideran al hacking como delito penal con pena de privativa de la libertad, argumentan que la experiencia es demostrativa que, en la mayoría de los casos, quien accede a un sistema informático intentará copiar información, destruirla, borrarla o apropiarse de algún dato valioso. Fundados en estudios criminológicos realizados en otros países que han demostrado que (en términos generales) los comportamientos que inicialmente se configuraron como de mero intrusismo informático, detectados pero no reprimidos por la legislación de ese momento, culminaron por pasar o dar paso a otros ilícitos más graves, como los diversos atentados a la intimidad, además del sabotaje, espionaje o defraudaciones informáticos. En función de ello, legislaciones como la de Estados Unidos optó por penalizar el mero intrusismo como un tipo residual, en la inteligencia de que ello actuaría como una suerte de *"delito barrera"* o *"delito obstáculo".*

Esta solución es la adoptada por la legislación argentina a partir de la Ley 26.388, en el art. 153 bis. En su redacción final, el tipo penal queda configurado con el mero acceso (indebido) a un dato o sistema de acceso restringido (sin exigencia de comprobación de daño real), y la pena que corresponde es de prisión (de 15 días a 6 meses).

Dentro de esta postura de sanción penal, otros autores consideran que caer en la pena privativa de la libertad para el hacking es excesivo, pensando en la posibilidad de los otros tipos de sanciones que incluye nuestro Código Penal en el art. 5, como la multa e inhabilitación (más allá de la responsabilidad civil que pudiere corresponder en el caso concreto).

2.8. Expansionismo penal y el riesgo de los delitos de peligro

Como se ha trabajado anteriormente, la pol, quedando el debate sobre la conveniencia o no de considerar a la pena privativa de la libertad como la más adecuada para el mismo.

En sus bases se observa que al afectar la confidencialidad (en todos los casos, siempre que el sistema sea restringido) y privacidad (en algunos casos), supone un riesgo para la información como interés colectivo. Dentro de este razonamiento, es entonces que se dan los fundamentos para su stura más aceptada en la actualidad, es la punición del hacking a través del derecho penal tipificación como delito de peligro abstracto, entendiendo que para su configuración, es suficiente la comprobación de la acción (acceso)[61].

Según Hassemer[62], los delitos de peligro abstracto facilitan la utilización del derecho penal, ya que no es necesario probar la lesión efectiva al bien jurídico, sino que solo basta con demostrar lo peligroso de la acción. Con ello reduce los requisitos para castigar y las posibilidades de defensa. Afirma que la criminalización de estas acciones, disminuyen el significado de derecho penal mínimo, y que es utilizado por el legislador para sus ganancias políticas. En derecho Penal, según el autor citado, ya no se trata de una respuesta adecuada a un hecho pasado, sino del dominio del futuro.

Con el fin de expresar una opinión crítica, opinamos que dicha postura es bastante peligrosa y potencialmente lesiva de garantías constitucionales. En esta línea Jiménez de Asúa, trabaja la idea que es una herramienta que debe ser manejada con cuidado y precisión, ya que la simple posibilidad no puede servir de índice para calificar como peligrosa una conducta humana. "*Al derecho penal solo le debe interesar un sector de la realidad, el que ofrece el riesgo más alto, pues si fuese a preocuparse de las mínimas posibilidades de amenaza a un interés o bien jurídico, la libertad humana recibiría un rudo golpe".* Por lo tanto, ha de exigirse la posibilidad inmediata o sea la probabilidad de lesión, que entendemos puede garantizarse a través de la inclusión de elementos subjetivos especiales del tipo penal.[63]

[61] BACIGALUPO, Enrique. "Manual de Derecho Penal". Editorial Temis. 1996, pág. 101

[62] HASSEMER, W. Rasgos y Crisis del Derecho Penal Moderno, Anuario de Derecho Penal y ciencias penales, 1992, págs.235-249

[63] JIMÉNEZ DE AZÚA *"Tratado de Derecho Penal"*, T. III, 1965, p. 472 ss.

Afirma el Dr. Carrión, que la tipificación del hacking necesariamente implicará la creación de un delito de peligro, por lo que, a los fines de zanjar las posibilidades de ataques constitucionales, propone dotarlo de elementos subjetivos en el ánimo del autor (dolo específico), que deben ser probados para formular el correspondiente reproche penal.[64]

En este punto consideramos que es importante sumar un reconocido principio penal denominado "Intervención Mínima de la Actuación Punitiva del Estado". Básicamente, este principio restringe el campo de la libertad y mediante la aplicación de una pena, priva de derechos fundamentales o condiciona su ejercicio. La característica propia es que, por un lado, debe ser el último de los recursos (*ultima ratio*) de los que el mismo tiene a su disposición para tutelar los bienes jurídicos y, por otra lado, debe ser lo menos gravoso posible para los derechos individuales, mientras resulte adecuado para alcanzar los fines de protección que se persiguen.

Esto implica que el Derecho Penal es la última barrera del Derecho, por lo que el legislador será quien deba evaluar si no existen otras medidas menos severas que puedan ser eficaces para lograr el objetivo (por ejemplo, la aplicación de sanciones administrativas, civiles, etc).

Se debe entender entonces que el carácter subsidiario del Derecho Penal frente a los demás instrumentos del ordenamiento jurídico y, así mismo, su carácter fragmentario, en cuanto no tutela todos los ataques a los bienes jurídicos relevantes sino únicamente a los que el legislador ha considerado como más graves.

La importancia de la comprensión de estos conceptos, radica esencialmente en que su confusión puede llevar a la proliferación de tipos penales especiales, en donde se presentan numerosos proyectos que pretenden condenar acciones que a simple vista parecen como disvaliosas, pero donde existen grandes dudas acerca de que es lo que realmente se está protegiendo. Este último comentario, viene referido a lo que algunos autores denominan el fenómeno de la expansión del derecho penal.

[64] CARRION, Hugo Daniel. "Presupuestos para la punibilidad del hacking", op. cit.

Siguiendo al maestro Jose María Silva Sanchez[65], citaremos las causas que a su criterio terminan por derivar en la expansión del derecho penal, toda vez que en una de ellas incorpora el concepto de ciberdelincuencia como fenómeno de ejemplo de sus teorías. Resumiendo brevemente, las causas de acuerdo a Silva Sanchez son:

1) Los nuevos intereses: *El derecho penal es un instrumento cualificado de protección de bienes jurídicos especialmente importantes. La expansión puede obedecer a la aparición de nuevos bienes jurídicos, por la conformación o generalización de nuevas realidades que antes no existían (ej: las instituciones económicas del crédito o la inversión) y por al deterioro de realidades tradicionalmente abundantes, que empiezan a manifestarse como bienes escasos (ej: el medio ambiente), así como por el incremento esencial de valor que experimentan ciertas realidades por el cambio social y cultural (ej: patrimonio artístico). En la actualidad es difícil encontrar consenso en la doctrina sobre cuáles de estos bienes jurídicos nuevos deben ser protegidos penalmente y en qué medida.*

2) La efectiva aparición de nuevos riesgos: *El modelo social postindustrial se ha caracterizado como "sociedad del riesgo". En este sentido, se configura el "riesgo de procedencia humana como fenómeno social estructural" donde gran parte de las amenazas a las que estamos expuestos los ciudadanos provienen de decisiones que otros ciudadanos realizan sobre el manejo de los avances técnicos. Por ello, aparecen nuevas técnicas como instrumentos para producir resultados lesivos y surgen modalidades delictivas dolosas de nuevo cuño (Ej; la ciberdelincuencia), pero además los avances tecnológicos inciden también en el ámbito de delincuencia no intencional: las consecuencias lesivas del "fallo técnico" y si éste debe ubicarse en el ámbito del riesgo penalmente relevante o bien en el propio del riesgo permitido.*

3) La institucionalización de la inseguridad: *La sociedad postindustrial es una sociedad de "objetiva inseguridad": los medios técnicos empleados, la comercialización de productos o la utilización de sustancias cuyos efectos*

[65] SILVA SANCHEZ, Jose María, "La expansión del derecho penal. Aspectos de la política criminal en las sociedades postindustriales. Editorial B de f, Montevideo – Buenos Aires. 2011

nocivos no se conocen, introducen un importante factor de incertidumbre en la sociedad. Además, existe una profunda interrelación de las esferas de organización individual, lo que incrementa la posibilidad de que algunos de estos contactos sociales redunden en la producción de consecuencias lesivas: recurso de los tipos de peligro y su configuración cada vez más abstracta y formalista. Asimismo, se producen de modo continuado fenómenos de transferencia y asunción de funciones de aseguramiento de esferas ajenas: tendencia hacia los delitos de comisión por omisión.

4) La sensación social de inseguridad: *Uno de los rasgos más significativos de las sociedades postindustriales es la "inseguridad sentida", la sensación general de inseguridad. La revolución del transporte y la actual de las comunicaciones da lugar a una falta de dominio del curso de los acontecimientos; las personas tienen dificultad de obtener una información fidedigna en una sociedad caracterizada por el alud de informaciones; el mercado mercantil y laboral reclama individuos solos y móviles, lo que produce una inestabilidad emocional-familiar. Todo esto se manifiesta en lo que ha denominado el vértigo de la relatividad: pérdida de referencias valorativas objetivas, ausencia de referencias o de principios generalizables, por lo que prevalece el pragmatismo del caso o la búsqueda de la solución consensuada. Esta inseguridad sentida suele ser un elemento de presión que observa al derecho como solución, y particularmente colaborando con el expansionismo penal.*

En conexión con la temática de la presente tesis, nos parece de suma importancia entender que parte de los "nuevos riesgos" trabajados por Silva Sanchez, son generados por la mala utilización de las nuevas tecnologías por parte de las personas. En este sentido es que afirma que aparecen nuevas técnicas como instrumentos para producir resultados lesivos y surgen modalidades delictivas dolosas de nuevo cuño, encontrándose aquí el corazón del concepto amplio de los delitos informáticos, que anteriormente desarrollamos.

A modo de reflexión personal sobre este fenómeno que muchas veces es valorado sólo desde un punto de vista negativo, consideramos que el derecho penal

debe ir adaptándose, con figuras cada vez más precisas y cuya persecución sea realmente consensuada a nivel social. Lo riesgoso, y aquí yace la importancia por la cuál es abordado este concepto y por el cual nos parece de interés acercarlo a este trabajo, es que en algunos casos esta expansión suele ser irrazonable, dando lugar a reclamos de un sector de la sociedad que parece entender que se vive en una situación de inseguridad (concepto absolutamente subjetivo), y que la "solución" a ello se encuentra a través del aumento de las penas, o bien, de la generación de nuevos tipos penales.

Consideramos un ejemplo del expansionismo que no suma, es la tipificación del art. 131 del Código Penal Argentino, considerando la figura del "grooming", criticado por diversos análisis[66], con una variedad de problemas importantes que terminan tornando a dicha figura prácticamente inaplicable, donde sigue siendo mucho más práctico aplicar la figura de corrupción de menores, que presenta mayor facilidad de prueba y una escala penal mayor adaptable al caso concreto.

2.9. Delitos informáticos y el bien jurídico protegido

Un tema de gran importancia para la temática abordada es un adecuado razonamiento acerca de cuál es el bien jurídico protegido en los delitos informáticos. ¿Podría acaso ser el bien jurídico protegido el común denominador entre tantos delitos que a simple vista parecen tan distintos?

Podría decirse que la doctrina ha esbozado tantas definiciones del bien jurídico protegido como autores han tratado el tema. No en vano dijo Welzel[67] que "el bien jurídico se ha convertido en un auténtico Proteo, que en las propias manos que creen sujetarlo se transforma enseguida en algo distinto".

[66] Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE), Investigación realizada por Daniela Schnidrig: "El delito de grooming en la legislación penal actual y proyectada en Argentina". Marzo 2016

[67] WELZEL, ZStW, 58, §. 491 ss., 509, cit. por JAKOBS, Günther, Derecho penal. Parte general. Fundamentos y teoría de la imputación, 2ª ed., trad. de Joaquín Cuello Contreras y José Serrano González de Murillo, Marcial Pons, Madrid, 1997 [2ª ed. alemana 1991], ps. 47 y 48

Por nuestra parte, y a modo de partir de un concepto moderadamente aceptado, seguiremos a Von Liszt, quien sostiene que el "bien jurídico" puede ser definido como un "*interés vital para el desarrollo de los individuos de una sociedad determinada, que adquiere reconocimiento jurídico*".

Superada la introducción conceptual, inicialmente existe un sector de la doctrina que los delitos informáticos no son una nueva categoría, sino que simplemente son los mismos delitos de siempre cometidos a través de nuevos medios. En estos casos, este sector entenderá que los bienes jurídicos protegidos son los mismos de siempre, que simplemente se han actualizado los tipos penales incluyendo nuevos medios de comisión, como bien podría ser el caso de las modificaciones del art. 153 y 153 bis de nuestro código penal[68].

Del otro lado de la balanza -como suele suceder en el derecho- existe una postura que considera que existe un nuevo bien jurídico a proteger que es la información, que tiene valor y que debe ser puesto en la escena penal de forma independiente a otros bienes jurídicos.

En palabras del Dr. Santiago Acurio Del Pino[69], "*podemos decir que el bien jurídico protegido en general es la información, pero considerada en diferentes formas, ya sea como un valor económico, como uno valor intrínseco de la persona, por su fluidez y tráfico jurídico, y finalmente por los sistemas que la procesan o automatizan; […] Por tanto el bien jurídico protegido, acoge a la confidencialidad, integridad, disponibilidad de la información y de los sistemas informáticos donde esta se almacena o transfiere*."

En la misma corriente podemos encontrar al Dr. Alexander Diaz García[70] quien reconoce que existe una tercera corriente que considera que los delitos informáticos deben ser observados desde un punto de vista triple: "*Como fin en si mismo, pues el computador puede ser objeto de la ofensa, al manipular o dañar la información que este pudiera contener; Como medio: Como herramienta del delito, cuando el sujeto*

[68] Modificación realizada por la Ley Nº 26.388

[69] DEL PINO, Santiago Acurio; "Generalidades de los delitos informáticos", Url: http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf,

[70] DIAZ GARCÍA, Alexander; "El bien jurídico tutelado de la información y los nuevos verbos rectores en los delitos informáticos", Url: http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

activo usa el ordenador para facilitar la comisión de un delito tradicional; Como objeto de prueba: Los computadores guardan pruebas incidentales de la comisión de ciertos actos delictivos a través de ellos.".

En relación con esta tercera postura expresamos que en realidad no sería una tercera corriente en sí, sino que esta perspectiva triple excede a la discusión sobre el bien jurídico protegido en sí, y en realidad expresa una posición sobre la propia categoría de los delitos informáticos, tema que ya hemos desarrollado anteriormente.

Volviendo al aporte realizado por el jurista colombiano Diaz García, quien participó en el proyecto y posterior sanción de la ley que incorpora los delitos informáticos en Colombia, en dicha norma (considerada una de las más modernas de nuestro continente), se agrega a la información como bien jurídico protegido en el esquema penal colombiano a través del art. 1[71] de la Ley 1273 de 2009.

Otro instrumento normativo que podemos citar como ejemplo, ya aquí de trascendencia internacional y probablemente el instrumento jurídico internacional más importante en materia de delitos informáticos -y al cuál prometemos dedicar algunas apreciaciones más adelante en esta tesis- es el Convenio de Cibercrimen de Budapest[72]. Por el momento y sin entrar en mayores detalles que serían necesarios para explicar dicho convenio, diremos brevemente que en el Capítulo II sobre medidas que deben adoptarse a nivel nacional, en la Sección 1 - Derecho penal sustantivo, el Título 1 se denomina "*Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos*".

Continuando con el tema del bien jurídico, considero apropiado abordar aquí una de las características de los delitos informáticos, que es que son pluriofensivos. Es decir, son delitos en los cuáles es posible encontrar la afectación de más de un bien jurídico a la vez.

---

[71] Artículo 1°. Adiciónase el Código Penal con un Título VII BIS denominado "De la Protección de la información y de los datos", del siguiente tenor: CAPITULO. I - "De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos"

[72] COUNCIL OF EUROPE. "Convenio de Cibercriminalidad de Budapest". Budapest, 23 de noviembre de 2001. Url: http://www.coe.int/t/dghl/standardsetting/t-cy/ETS_185_spanish.pdf , Consultado: : 10 de Abril de 2017

A modo de ejemplo, podemos citar el caso del hurto, un delito que afecta en principio únicamente a la propiedad, mientras que si fuera un caso de robo, al exigir la violencia, puede afectar también a la integridad física de las víctimas. En el caso de algunos de los delitos informáticos, nos encontramos ante una situación similar, pero con distintos bienes jurídicos.

Para los autores chilenos Claudio Magliona y Macarena López[73], los delitos informáticos tienen el carácter de pluriofensivos o complejos, es decir "*que se caracterizan porque simultáneamente protegen varios intereses jurídicos, sin perjuicio de que uno de tales bienes está independientemente tutelado por otro tipo*"

En el caso de los delitos informáticos, una estafa electrónica puede afectar por un lado la confidencialidad de la información, su integridad, el patrimonio y depende del sistema atacado, hasta ser también delitos que ataquen el orden económico y financiero gubernamental.

En palabras del Dr. Magliona Markovicth y López Medel, la tecnología está proporcionando nuevos elementos para atentar contra bienes ya existentes (intimidad, seguridad nacional, patrimonio, etc.), sin embargo han ido adquiriendo importancia nuevos bienes, como sería la calidad, pureza e idoneidad de la información en cuanto tal y de los productos de que ella se obtengan; la confianza en los sistemas informáticos; nuevos aspectos de la propiedad en cuanto recaiga sobre la información personal registrada o sobre la información nominativa.

A modo de corolario de esta temática, consideramos de importancia para el tema en sí, toda vez que el no consenso sobre el bien jurídico protegido terminar por derivar en problemas de aplicación final de los tipos penales.

Adherimos que debe ser la información un nuevo bien jurídico protegido, como un bien intangible pero de claro valor en nuestra precisamente "Sociedad de la Información". Sin embargo, debemos puntualizar que aspectos de la información consideramos importante para proteger. ¿Acaso es cualquier tipo de información susceptible de recibir el resguardo del arma más dura que tiene el derecho, el sistema penal?

---

[73] MAGLIONA MARKOVICTH Claudio Paúl, LÓPEZ MEDEL Macarena, Delincuencia y Fraude Informático, Editorial Jurídica de Chile. 1999

Consideramos dicha respuesta como negativa, entendiendo que no cualquier información debería ser protegida, o para ser más preciso, no cualquier aspecto de la información debería ser protegido. En este sentido, observamos que los aspectos de la información a ser considerados con valor jurídico son: la confidencialidad, la integridad y la disponibilidad de la información, es decir, los tres pilares de la seguridad de la información desarrollados anteriormente.

Desde esta óptica, será posible entender por ejemplo que, en el caso de acceso indebido a un sistema informático, el bien jurídico afectado podría ser la confidencialidad de la información (violación de secretos). En el caso de daño informático (sabotaje para algunos autores), se afectaría la integridad de la información. En el caso de la denegación de servicios, el bien jurídico afectado sería la disponibilidad de la información. Los ejemplos dados son con fines didácticos, ya que como se ha visto, muchos de estos delitos son pluriofensivos, por lo que, en el caso concreto, más allá de la afectación de estos valores de la información, además podrían ser afectados otros tantos (intimidad de una persona, patrimonio, entre otros).

2.10. Caracteres de los delitos informáticos

Antes de pasar a un desarrollo más pormenorizado de distintos desafíos que plantean los delitos informáticos, parece atinado citar a otro maestro del Derecho Informático y autor de la primera obra relacionada al tema en nuestro país, el Dr. Horacio Fernández Delpech[74], quien en su última actualización de su obra realiza un detalle sobre serie de circunstancias que hacen que este tipo de ilícitos penales sean de difícil represión:

1. *La falta de una tipificación específica en la mayoría de las legislaciones de los delitos informáticos y cometidos a través de la red;*

[74] FERNANDEZ DELPECH, Horacio, Manual de Derecho Informático, 1ra. Edición, Ed. Abeledo Perrot, Argentina, 2014, Pág. 194

2. *La transnacionalidad de las conductas, que muchas veces se realizan en un país, pero cuyos resultados se producen en otro;*
3. *La falta de consenso internacional sobre la reprochabilidad de ciertas conductas;*
4. *Las permanentes innovaciones tecnológicas, que generalmente avanzan más rápido que las implementaciones de soluciones normativas;*

Como se observa, el Dr. Fernandez Delpech nos trae una primera serie de características propias de los delitos aquí en estudio, entre las que podemos encontrar la transnacionalidad, la falta de legislación adecuada y la falta de coordinación penal entre los países, aspectos que a continuación desarrollaremos.

En palabras de Pablo Palazzi, uno de los autores más reconocidos en la materia penal informática, "*cabe resaltar la magnitud de los daños, la cada vez más frecuente naturaleza global e internacional de esta clase de delitos; la facilidad para cometerlos; y las dificultades para la investigación, que ha llevado a la necesidad cada vez mayor de cooperación entre fuerzas de seguridad y el sector privado por la necesidad de preservar datos en el tráfico de ISP, servidores y finalmente, las empresas de hosting y numerosas reconfiguraciones de los esquemas tradicionales con los cuales se concibe el derecho penal*".[75]

Otro autor que se anima a indicar características propias es el Dr. Julio Tellez Valdez[76], a quien ya hemos citado anteriormente al momento de la conceptualización de los delitos informáticos. Según Tellez Valdez, este tipo de delitos presentan las siguientes características principales:

1. *Son conductas criminales de cuello blanco (white collar crime), en tanto que sólo un determinado número de personas con ciertos conocimientos (en este caso técnicos) puede llegar a cometerlas.*
2. *Son acciones ocupacionales, en cuanto a que muchas veces se realizan cuando el sujeto se halla trabajando.*

[75] PALAZZI, Pablo Andrés, "Delitos Informáticos", Ad-Hoc, Buenos Aires, 2000.

[76] Op. Cita 29

3. *Son acciones de oportunidad, ya que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico.*
4. *Provocan serias pérdidas económicas, ya que casi siempre producen «beneficios» de más de cinco cifras a aquellos que las realizan.*
5. *Ofrecen posibilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a consumarse.*
6. *Son muchos los casos y pocas las denuncias, y todo ello debido a la misma falta de regulación por parte del Derecho.*
7. *Son muy sofisticados y relativamente frecuentes en el ámbito militar.*
8. *Presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico.*
9. *Tienden a proliferar cada vez más, por lo que requieren una urgente regulación. Por el momento siguen siendo ilícitos impunes de manera manifiesta ante la ley.*

A modo de cierre del presente capítulo, y con fines metodológicos intentaremos, tomando como base varias de las características citadas por estos autores, realizar un breve desarrollo, crítica y reflexión aquellas características que a nuestro criterio, debemos repensar para comprender la problemática del ciberdelito:

2.10.1 Delitos de cuellos blanco

Tradicionalmente se ha considerado que los delitos informáticos estarían incluídos dentro de la categoría denominada “de cuello blanco” (*white collar crimes*), toda vez que los mismos sólo podían ser realizados por aquellas personas con profundos o avanzados conocimientos en sistemas de información. A nuestro criterio, consideramos que en la actualidad es una categoría que no parece ser tan exacta para este tipo de delitos, toda vez que la evolución en materia de (in)seguridad informática ha llevado que los conocimientos sean cada vez más

accesibles y difundidos, y las posibilidades de acceder a *rootkits*[77], incluso de forma gratuita y al alcance de un par de clicks, termina generando toda una nueva generación de ciberdelincuentes que ya no poseen grandes conocimientos sobre el funcionamiento de un sistema, sino que solamente son ejecutores de herramientas realizadas por terceros.

El cibercrimen como negocio demanda un aumento de ataques, que son realizados de forma masiva a todas partes del mundo (característica que se analiza a continuación), y por lo tanto, la necesidad de los ataques alienta la generación de herramientas que realizan todas las tareas de forma automatizada.

Como consecuencia existe una gran cantidad de ciberdelincuentes que utilizan estas herramientas, pero que realmente no comprenden todo el conocimiento que hay en la construcción de la misma, ni saben cuál es la vulnerabilidad explotada, ni la forma en que se explota o se escalan los privilegios, ni tampoco les interesa.

Por todo lo expuesto, consideramos que actualmente la aplicación de la categoría de "delitos de cuello blanco" si bien dependerá del tipo de delito informático analizado, por lo general ya son delitos que pueden ser llevados a cabo por cualquier persona que invierta el dinero suficiente para conseguir las herramientas necesarias.

2.10.2 Trasnacionales

La posibilidad tecnológica de las comunicaciones a distancia a través de las redes, conciben la posibilidad que la persona que delinque se encuentre físicamente alejado (incluso en otro país) de la víctima.

La transnacionalidad como propiedad de los delitos informáticos, implica que los mismos no encuentran barreras jurisdiccionales para llevarse a cabo. Es decir que, técnicamente es posible estar conectado a una red en Argentina, pasar por un router[78] conectado en Rusia, utilizar una botnet[79] de computadoras en Colombia y

[77] Op. cita 53

[78] Un *router* o enrutador, es un dispositivo que proporciona conectividad a nivel de red.

[79] Una *botnet* es una red de computadoras "zombies", es decir que han sido previamente infectadas y que permiten que quien tenga su control, pueda utilizarlas como armas para distintos tipos de ataques.

finalmente atacar un sistema en Cuba. Por más complejo que pueda parecer en el relato, técnicamente es de relativa facilidad, siempre que se cuente con un mínimo de conocimientos técnicos.

Esta característica es de relevancia ya que en el caso del cibercrimen, muchas bandas organizadas suelen realizar los delitos desde países -por ejemplo, Rusia, Moldavia, Rumania, etc- cuyas características propias -complicaciones de idioma, falta de legislación en la materia, falta de cooperación internacional para la justicia, entre otros- hacen que las investigaciones sea de alto nivel de complejidad (aspecto que analizaremos más adelante en este listado de características propias).

Estos casos vuelven a poner sobre las mesas de los debates académicos las clásicas preguntas sobre la legislación aplicable, pero sobre todo postula el claro desafío de coordinar distintos ámbitos de colaboración internacional.

Este es un tema clave, toda vez que cada Estado deberá de una forma u otra establecer sus posturas en relación a los límites o avances en las investigaciones de delitos (informáticos en nuestro caso) a nivel internacional. Esta decisión, excede el ámbito jurídico de esta tesis, pero dejamos cuenta que su profundización responde a cuestiones de política internacional como uno de los aspectos claves para las relaciones internacionales.

La potencial afectación de la soberanía de otro Estado, que podemos observar en las discusiones realizadas en torno al acceso transfronterizo de datos, al cuál dedicaremos algunos párrafos adelantando que su complejidad también excede del objeto de esta tesis.

la cooperación eficiente e igualitaria entre Estados, la protección de garantías individuales en entornos digitales, la relación con las empresas multinacionales del sector de la informática y las telecomunicaciones, entre otros.

En relación con este último aspecto, el Convenio de Cibercriminalidad de Budapest[80], que abordaremos más adelante, es considerado el instrumento internacional más importante en la materia precisamente porque apunta a tener dentro de los Estados firmantes, un mínimo de coordinación en el ámbito penal material, y un potente marco de cooperación internacional (procesal penal) para casos de cibercrimen.

No obstante la ya citada necesidad de cooperación internacional, consideramos de relevancia marcar la necesidad de un previo marco de cooperación a nivel nacional en Argentina. Dicha observación radica en que en la actualidad se pueden observar diferentes realidades en nuestro país, cada una de ellas dependiendo del grado de desarrollo y poderío económico de cada Provincia en particular. A modo de ejemplo y comparación, el mismo delito ocurrido en Buenos Aires, donde poseen la posibilidad de denuncia ante la División de Delitos Tecnológicos de la Policía Federal Argentina o ante el Área Especial de Investigaciones Telemáticos de la Policía Metropolitana, no tiene las mismas posibilidades y recursos para ser investigados que si es denunciado en la Provincia de Corrientes, Formosa, o incluso Santa Fe.

En consecuencia de la heterogeneidad de situaciones hacia el interior de nuestro país, consideramos que más allá de promulgar una mejor cooperación a nivel internacional, también tengamos en cuenta la necesidad de generación de una "Red Nacional de Cooperación en materia de Delitos Informáticos", para que aquellas Provincias (como por ejemplo la Provincia de Santa Fe) que aún no tienen una estructura armada en la materia, puedan acceder a los avances y experiencias de otras con mayor desarrollo en el área (tales como Buenos Aires y Córdoba), con la posibilidad de acceder y conocer canales ágiles de cooperación para los casos que requieran colaboración interjurisdiccional.

2.10.3 Instantáneos

Esta característica tiene más bien que ver con algo propio de las nuevas tecnologías (al igual que la comisión a distancia), toda vez que, más allá del tiempo

[80] COUNCIL OF EUROPE. "Convenio de Cibercriminalidad de Budapest". Budapest, 23 de noviembre de 2001. Url: http://www.coe.int/t/dghl/standardsetting/t-cy/ETS_185_spanish.pdf, Consultado: 27 de Junio de 2017

que podría llevar una eventual inteligencia preliminar o preparación de un ataque determinado, la ejecución del delito suele ser instantánea.

Es decir, por lo general el momento de perfeccionamiento del delito se da en el propio momento en que el delincuente lleva adelante la acción, consumiéndose en el propio acto. Pensemos como ejemplo, casos de accesos indebidos a sistemas o datos restringidos -hacking-, daños informáticos (como la eliminación de un dato).

Afirmamos que no todos los delitos informáticos son instantáneos, toda vez que existen casos que podríamos considerar que no se consumen en el acto, sino que permanecen en el tiempo, tales como un caso de denegación de servicio, donde por ejemplo un sistema informático quedará fuera de servicio por unas horas. Asimismo podría considerarse el caso de un ataque de ransomware, toda vez que la primera fase de cifrado de información suele llevar un tiempo prolongado, y mientras dicha información permanezca “secuestrada”, también podría considerarse la continuación del mismo.

2.10.4 Masivos o Simultáneos

Esta característica tiene que ver con la posibilidad de la comisión de los delitos informáticos puedan ser realizados de forma simultánea. Esto tiene relación directa con las posibilidades tecnológicas de:

- Difusión masiva de contenidos dañinos
- Ataques automatizados

En el primero de los casos, y a modo de ejemplo podemos mencionar los casos de spam con ataques de phishing masivo o casos de envío masivo de correos electrónicos que esconden entre sus adjuntos malware -código malicioso- listo para infectar los equipos de las víctimas.

De esta forma, la posibilidad de contar con servicios que permiten el envío masivo de mensajes electrónicos (ya sean correos electrónicos, sms, whatsapp, etc), permite al delincuente, llegar a más potenciales víctimas en menos tiempo.

En el segundo de los casos, el aumento en la generación de herramientas que automatizan el proceso de detección de sistemas vulnerables, junto con su explotación e infección posterior, permite que los delincuentes dejen corriendo

procesos de ataques masivos alrededor del mundo, buscando víctimas que no han tomado los recaudos de seguridad de la información necesarios, como por ejemplo, la actualización de sus sistemas operativos, como ocurrió en el conocido caso de Wannacry[81].

2.10.5 Anónimos

Con esta característica nos referimos a la posibilidad del delincuente de lograr obtener distintos niveles de anonimato, gracias a la utilización de tecnologías dedicadas a la materia. Es decir, que la persona que las utiliza puede ocultar su verdadera identidad, o en el caso de las redes, el lugar real desde el cual está conectándose para llevar adelante sus acciones.

El primer comentario que nos interesa destacar respecto a la temática es que el anonimato no debe ser tomado en sí como solamente negativo, cayendo en la demonización de las herramientas que permiten lograr los distintos niveles de anonimato.

Entendemos que el anonimato es necesario toda vez que permite que muchas personas que se encuentran en contexto de persecución o censura, puedan ver efectivizados sus derechos de libre acceso a la información y libre expresión en las redes, gracias a estas tecnologías que permiten evitar exponer el lugar real desde donde se están conectando a la red.

Como hemos sostenido en el primer capítulo de este trabajo, adherimos a la posición sobre que las tecnologías son neutras y su valoración dependerá pura y exclusivamente de lo que la persona en sí decida hacer con ellas.

En el caso de la comisión de delitos informáticos, las distintas técnicas de anonimato existentes -en el caso que sean utilizadas- llevan al investigador a enfrentarse con una misión difícil al momento de intentar determinar al autor de un delito.

Nos parece importante destacar que ninguna tecnología es 100% segura, y en consecuencia, tampoco ninguna tecnología podría garantizar un 100% de

[81] SEGU-INFO; "Wannacry: al menos 75 países afectados", URL: http://blog.segu-info.com.ar/2017/05/wannacrypt-al-menos-15-paises-afectados.html

anonimato. En esta línea, consideramos que desde lo técnico-jurídico, es más correcto hablar de "niveles" de anonimato que, dependiendo del tipo de tecnología, implicarán un desafío mayor o menor para el investigador.

A modo de ejemplo breve, que será mejor desarrollado en el apartado dedicado a la investigación del delito, no es el mismo nivel de anonimato un delito cometido desde un wifi público (un nivel bajo de anonimato) que un delito cometido utilizando la red TOR (cifrado tipo cebolla), que es mundialmente conocida por ser una de las puertas de entrada para la Deep Web.

Sobre el tema "Deep Web" pueden encontrar una importante cantidad de artículos[82], publicados en diversos medios, algunos incluso diarios de importantes nombres[83], donde se brindan estadísticas sobre la cantidad de contenidos y se afirman determinados datos que no poseen ningún tipo de fuente, o al menos, si las supuestas fuentes existen, la información no se encuentra adecuadamente fundada, no al menos desde el punto de vista académico o científico.

De nuestra parte, hace algunos años y considerando la importancia del tema y el interés que el mismo representa para este autor, se ha tenido la posibilidad de escribir un artículo académico dedicado sobre Deep Web, anonimato y Cibercrimen[84], donde hemos desarrollado la relación existente entre el anonimato y el incremento del cibercrimen en la sociedad de la información.

La Deep Web es un espacio virtual más que existe en la actualidad, cada vez más accesible para los usuarios, y que posee determinadas características que es necesario considerar si se quiere hacer un estudio completo sobre los delitos .

Esta Deep web, o Internet profunda, o Internet oculta no es más que una parte de la red de Internet en la cuál los contenidos no son indexados por los motores de

---

[82] TELAM, "La Internet Profunda, adonde navega el delito", Url: http://www.telam.com.ar/notas/201705/189791-internet-profunda-deep-web-delito.html, Consultado: 12 de Junio de 2017

[83] DIARIO CLARÍN, "Sicarios, drogas y pornografía infantil, los delitos que esconde la Dark Web", Url: https://www.clarin.com/suplementos/zona/sicarios-drogas-pornografia-infantil-delitos-esconde-dark-web_0_BJ9DTYe7b.html, Consultado: 12 de Junio de 2017

[84] TEMPERINI, Marcelo; "Deep web, anonimato y Cibercrimen". VI Congreso Iberoamericano de Investigadores y docentes de Derecho e Informática (CIIDDI 2016). ISBN: 9789876921381, 2016.

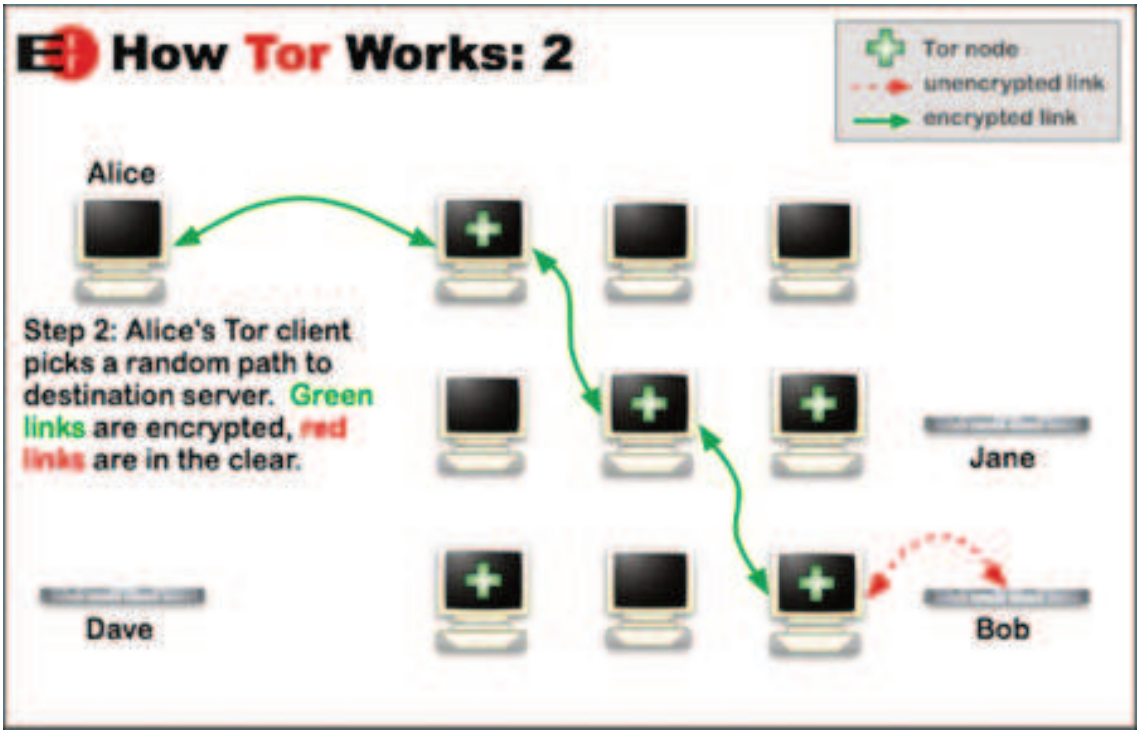
búsquedas tradicionales (Google, Yahoo, etc.). Por ello y en contraste con la Deep Web, Internet como la conocemos se la conoce también como Internet superficial.

Los contenidos pueden no ser indexados por ejemplo porque son páginas web dinámicas, sitios bloqueados (por un CAPTCHA por ejemplo), sitios sin linkear, sitios privados (acceso sólo con credenciales), sitios con contenidos que no son HTML o contextual, así como redes de accesos limitados (por ejemplo, a determinados protocolos de accesos).

Dentro de estos últimos, de contenidos que sólo son accesibles a través de un determinado software o protocolo específico, podemos encontrar al Proyecto TOR[85], una de las herramientas más conocidas, que construye un circuito de conexiones cifradas a través de repetidores en la red.

El circuito se extiende un salto a la vez, y cada nodo a lo largo del camino conoce únicamente el nodo que le proporciona los datos y retransmitir los cuales se los entrega. De esta forma, un nodo de forma individual nunca conoce el recorrido completo que ha tomado un paquete de datos. El cliente negocia un paquete separado de claves de cifrado para cada tramo a lo largo del circuito, asegurando que la información circulante entre los nodos no pueda ser rastreada.

[85] Creado en 2003 por Roger Dingledine, Nick Mathewson y Paul Syverson surgió como la evolución del proyecto Onion Routing del Laboratorio de Investigación Naval de los Estados Unidos. A finales de 2004 pasó a ser patrocinado por la Electronic Frontier Foundation, la organización de defensa de libertades civiles en el mundo digital, hasta noviembre de 2005. Actualmente el proyecto Tor está en manos del 'Tor project' una organización sin ánimo de lucro orientada a la investigación y la educación, radicada en Massachusetts y que ha sido financiada por distintas organizaciones. Es un proyecto cuyo objetivo principal es el desarrollo de una red de comunicaciones distribuida de baja latencia y superpuesta sobre internet, en la que el encaminamiento de los mensajes intercambiados entre los usuarios no revela la identidad de la conexión (dirección IP) permitiendo un anonimato a nivel de red y que, además, mantiene la integridad y el secreto de la información que viaja por ella. Para la consecución de estos objetivos se ha desarrollado un software libre específico, donde propone el uso de una ruta de conexión del tipo “cebolla”, es decir donde los mensajes viajen desde el origen al destino saltando a través de distintos routers ubicados en distintos puntos del mundo, generando un sistema de protección de la identidad de varias capas (de allí sale el nombre de cebolla). Más información en https://www.torproject.org



El circuito de conexión a través de tres nodos distintos, cambia cada aproximadamente diez minutos, dificultando aún más cualquier intento de análisis o crackeo de las conexiones circulantes por los nodos.

Todo el esfuerzo fue premiado en marzo de 2011, cuando TOR recibió de la Free Software Foundation el premio para proyectos de beneficio social correspondiente a 2010 por "*haber permitido que, aproximadamente, 36 millones de personas de todo el mundo, usando software libre, hayan experimentado libertad de acceso y de expresión en Internet manteniendo su privacidad y anonimato. Su red ha resultado crucial en los movimientos disidentes de Irán y Egipto*"[86].

2.10.6 Pluriofensivos

Hemos ya señalado anteriormente que estamos ante delitos en los cuáles es posible encontrar la afectación de más de un bien jurídico a la vez, es decir, que pueden ser dependiendo del caso, pluriofensivos[87].

[86] CENATIC, "Premian a Tor Project por su protección del anonimato en la red", Url: http://www.cenatic.es/hemeroteca-de-cenatic/3-sobre-el-sector-del-sfa/39348-premian-a-tor-project-por-su-proteccion-del-anonimato-en-la-red?format=pdf, Consultado: 12 de Junio de 2021

[87] Cornejo Arismendi, J. Criminalidad Informática y la Discusión Sobre el Bien Jurídico Protegido en los Delitos Informáticos.

En el caso de los delitos informáticos y a modo didáctico citaremos un caso sobre un ataque informático contra el sitio web del Ejército Argentino[88], en la cuál se inscribieron consignas vinculadas al grupo terrorista ISIS[89]. En principio y de acuerdo a la información disponible se trata de un ataque conocido como un *deface*[90] de un sitio web, que desde un punto de vista jurídico puede ser considerado como un caso de daño informático (art. 183 2do. Párrafo), toda vez que en el bien jurídico afectado sería la la confidencialidad y la integridad de la información (que no sólo fue accedida ilegítimamente, sino que además fue alterada). A su vez, podríamos considerar que podría existir -en el caso citado de la web del Ejército Argentino-, un delito que podría comprometer la Seguridad de la Nación, como aquellos delitos contra la paz y la dignidad de la Nación[91].

Otro caso que puede ilustrar de forma sencilla para el lector sobre aspecto pluriofensivo de un delito informático, es un caso de una estafa electrónica donde la víctima es engañada por un ataque de phishing. Si bien en principio podemos observar una afectación a la confidencialidad de la información por un lado (en relación a sus datos bancarios), afectación del patrimonio (con la estafa en sí), y depende del sistema atacado, podría también considerar que el mismo delito podría estar comprometiendo o atacando el orden económico y financiero[92].

A modo constructivo, al momento de la cita de diferentes autores hemos citado a varios que entre sus características señalaba que los delitos informáticos

---

[88] DIARIO LA NACIÓN, "Hackean con una leyenda de la web del Ejército", Url: http://www.lanacion.com.ar/2035198-hackean-con-una-leyenda-de-ei-la-web-del-ejercito", Consultado: 20 de Junio de 2017

[89] En el sitio web del Ejército, podía leerse "Somos el Estado Islámico ALLAHU AKBAR. - Esto es una amenaza. ISIS está en Argentina y muy pronto van a saber de nosotros. Allahu Akbar".

[90] El defacing es la práctica de, sin consentimiento de sus legítimos titulares, modificar o alterar la portada de un sitio web, web de un sitio. Los motivos de esta práctica (muy común en el ambito de la seguridad informática), suelen ser por cuestiones ideológicas (buscan dar un mensaje), políticas, religiosas, y en algunos casos, simplemente por diversión de los atacantes, para quienes la captura de pantalla del deface, sirve en muchos casos como una "medalla" para colgarse que tiene cierto valor en un sistema de meritocracia.

[91] CODIGO PENAL DE LA NACION ARGENTINA; LEY 11.179; TITULO IX: DELITOS CONTRA LA SEGURIDAD DE LA NACION; Capítulo II: Delitos que comprometen la paz y la dignidad de la Nación.

[92] VEREAU, Renzo Vinelli. Los delitos informáticos y su relación con la criminalidad económica. *Ius et Praxis*

"*provocan serias pérdidas económicas y que generan para el delincuente beneficios de más de cinco cifras*". En relación a estas afirmaciones, nos permitimos realizar algunas observaciones.

En primer lugar, no consideramos correcto relacionar exclusivamente a los delitos informáticos con los daños directamente económicos, toda vez que muchos de ellos afectan la intimidad, privacidad, honor, reputación, e incluso hasta la integridad o normal desarrollo sexual de los menores -casos de grooming-. En esta línea, opinamos que los grandes (o conocidos) informes sobre cibercrimen a nivel mundial (Symantec, Panda, TrendMicro, entre otros), tienden a realizar estas asociaciones económicas sobre el cibercrimen ya que buscan generar en el lector -potenciales clientes de los servicios de prevención en materia de seguridad informática que esas mismas empresas ofrecen- de dichos informes, una generación de concientización sobre su propia inseguridad informática que tenga por consecuencia la justificación de la inversión que deberían realizar para mejorar los niveles de seguridad de sus sistemas de información.

En segundo lugar, también nos permitimos dudar de la afirmación de que los beneficios superan las cinco cifras, toda vez que incluso en aquellos delitos informáticos cuyo objetivo directo es la afectación del patrimonio de la víctima (como las estafas electrónicas), salvo excepciones, por lo general suelen ser de poco monto (conocido de modalidad hormiga) a fin de que la víctima no se de cuenta y el fraude se mantenga la mayor cantidad de tiempo posible. Si bien, la suma de todos esos delitos informáticos que afectan el patrimonio, podría ser enorme, el nivel actual de cifra negra existente en la materia (aspecto fundamental que analizaremos en esta tesis), impide tener certeza sobre la verdadera magnitud del daño.

A modo de cierre sobre este aspecto, consideramos que uno de los grandes desafíos / problemas de los delitos informáticos es la dificultad que exista en la cuantificación del daño (tomando un concepto del derecho de daños), toda vez que muchos de los bienes jurídicos afectados son subjetivos (dignidad, honra, reputación, buen nombre, etc.). Incluso con la propia información, es difícil realizar una tasación cierta de cuánto vale la información que uno posee, ya que siempre dependerá del tipo de información de que se trate y sobre todo, del valor personal que tenga la misma.

Capítulo III: Estadísticas en ciberdelincuencia

3.1. Introducción

Medir el impacto del delito cibernético permite que todo el espectro del sistema de justicia penal pueda generar políticas y respuestas operativas más efectivas. Por otro lado, también permite la movilización basada en evidencia y la alineación de recursos.

Analizar adecuadamente las cifras y tendencias, permite que las autoridades de justicia penal puedan tener una mejor idea de sus propias capacidades y áreas de mejora.

En este contexto, el Consejo de Europa e INTERPOL han desarrollado conjuntamente la Guía para estadísticas de justicia penal sobre delitos cibernéticos y evidencia electrónica para ayudar a los países a compilar estadísticas de manera eficiente[93]. El objetivo principal de esta guía es apoyar a las autoridades de justicia penal en la introducción de estadísticas sobre delitos cibernéticos y pruebas electrónicas proporcionando buenas prácticas y recomendaciones, fomentando por un lado la generación de estadísticas pero también alentando a su difusión.

Uno de los fenómenos que se intentan combatir a través de este tipo de guías, es la proliferación de distintas metodologías y procedimientos al momento de realizar las estadísticas, que implicaría un obstáculo al momento de realizar comparativas o compartir información acerca de la situación existente en un determinado momento en relación a la ciberdelincuencia.

[93] INTERPOL, Council of Europe & European Union: “Guide for Criminal Justice Statistics on Cybercrime and Electronic Evidence”, 2020. Url: https://cybilportal.org/publications/guide-for-criminal-justice-statistics-on-cybercrime-and-electronic-evidence/

Abordaremos también algunos estudios previos que destacan los niveles de cifra negra en los delitos informáticos, con su posterior análisis sobre cuáles son los factores y causas que se esconden detrás de este fenómeno.

Entendemos entonces que la existencia de estadísticas sobre delincuencia informática resulta un aspecto esencial para dar lugar a la adopción de políticas adecuadas por parte del Estado. En contrapartida, la escasez de datos más próximos a la realidad que acontece sobre la problemática, impide avanzar en la toma de decisiones de política criminal importantes a mediano o largo plazo.

3.2 Estadísticas corporativas

Como hemos adelantado, a lo largo de este capítulo iremos identificando los distintos estudios que existen al respecto, que nos brinden mayores datos acerca de estadísticas que permitan visibilizar o dimensionar la verdadera magnitud de este flagelo.

Comenzaremos esta empresa abordando algunos de los índices más relevantes (al menos al momento de la generación de estas líneas) informados por el ámbito privado de la seguridad de la información.

De acuerdo a un informe internacional de Norton, una reconocida empresa de ciberseguridad, las víctimas de delitos informáticos aumentaron de un 10% a un 13% entre 2011 a 2012[94].

Por otro lado y conexión directa, Panda Security afirma el crecimiento sostenido del mercado negro de la información[95], que funciona como motor que impulsa una importante masa de ataques informáticos, principalmente destinados a obtener bases de datos con información personal.

De acuerdo a uno de los estudios de mayor relevancia mundial en delitos informáticos, realizados por la empresa de ciberseguridad Symantec[96], en el cuál se

[94] NORTON, "Informe sobre delitos informáticos" 2011, URL: http://norton.com/cybercrimereport.

[95] PANDA SECURITY. The Cyber-Crime Black Market. 2011. Url: http://cybercrime.pandasecurity.com/blackmarket. Consultado: 28/06/2017

[96] SYMANTEC CORPORATION, "Informe de Norton sobre delitos informáticos para el año 2012", Url: http://www.norton.com/2012cybercrimereport

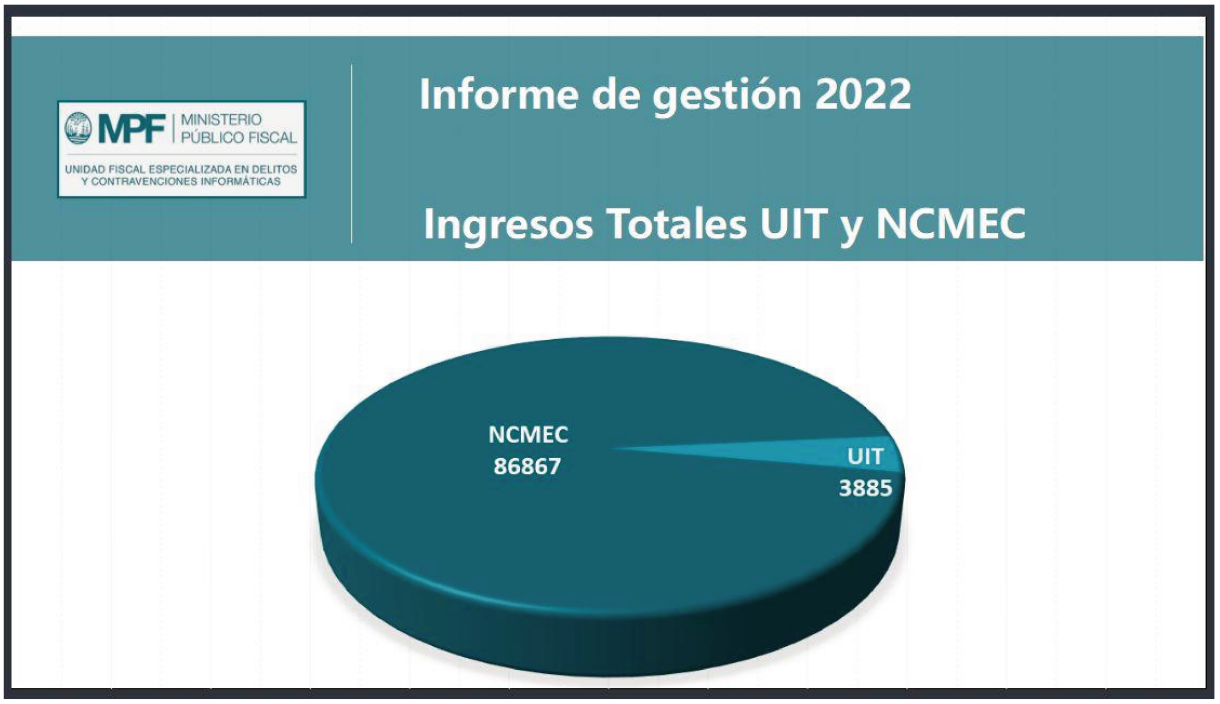
han entrevistado más de 13.000 adultos en 24 países, para el año 2012, se calculó que los costos directos asociados con los delitos informáticos que afectan a los consumidores en el mundo ascendieron a US$ 110.000 billones en doce meses.

El mismo estudio revela que por cada segundo 18 adultos son víctimas de un delito informático, lo que da como resultado más de un millón y medio de víctimas de delitos informáticos cada día, a nivel mundial.

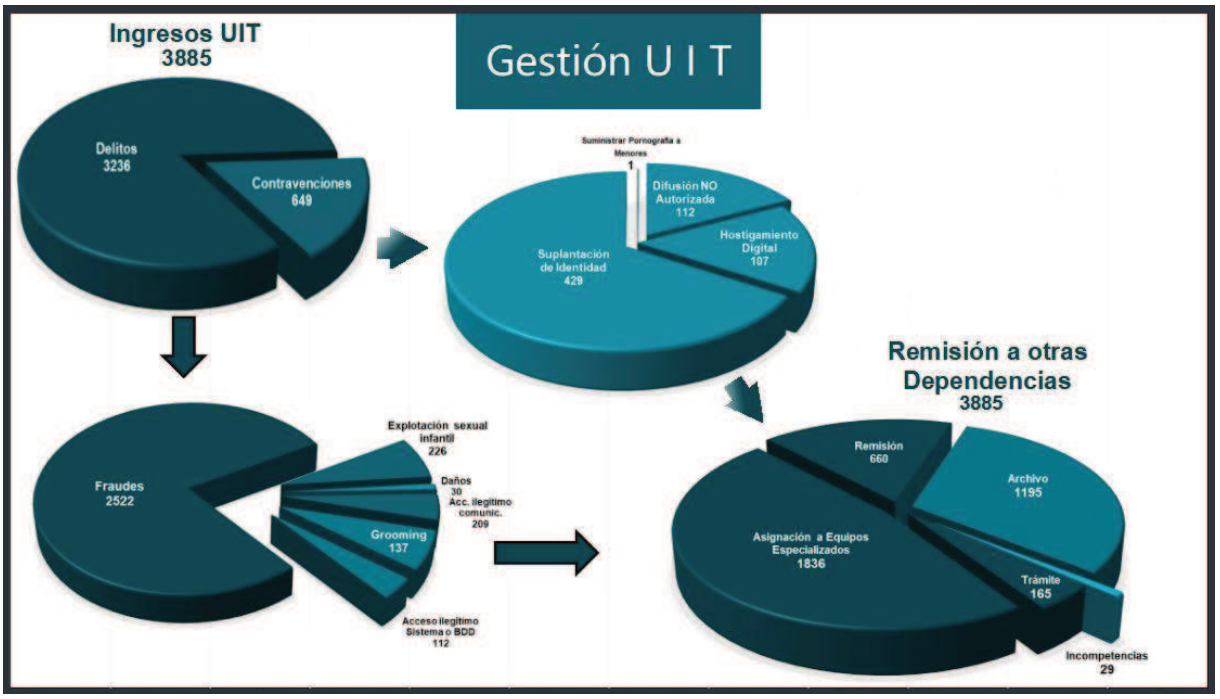
3.3 Estadísticas oficiales a nivel nacional.

3.3.1. Estadísticas anuales de la UFEDYCI

De acuerdo al informe de gestión realizado por la Fiscalía Especializada en Delitos y Contravenciones Informáticas, dirigida por la Dra. Daniela Dupuy, durante el año 2022 se han realizado una importante cantidad de investigaciones, cuyos resumen de datos publicados se comparten a continuación.



En principio se puede observar que durante el año 2022, ingresaron 86867 casos desde NCMEC[97] y 3885 de la Unidad de Intervención Temprana (UIT).



De esos 3885 casos de la UIT, se desprende que 3236 fueron considerados delitos mientras que los restantes 649 casos han sido contravenciones (recordemos que dichas fiscalías son tanto de delitos como de contravenciones).

En relación a los delitos recibidos, 2522 han sido casos de fraudes[98] (casi un 78% de la totalidad de los delitos), 226 casos de explotación sexual infantil, 30 casos de daño, 209 casos de acceso ilegítimo a comunicaciones privadas, 137 casos de grooming y 112 casos de acceso ilegítimos a sistemas o bases de datos.

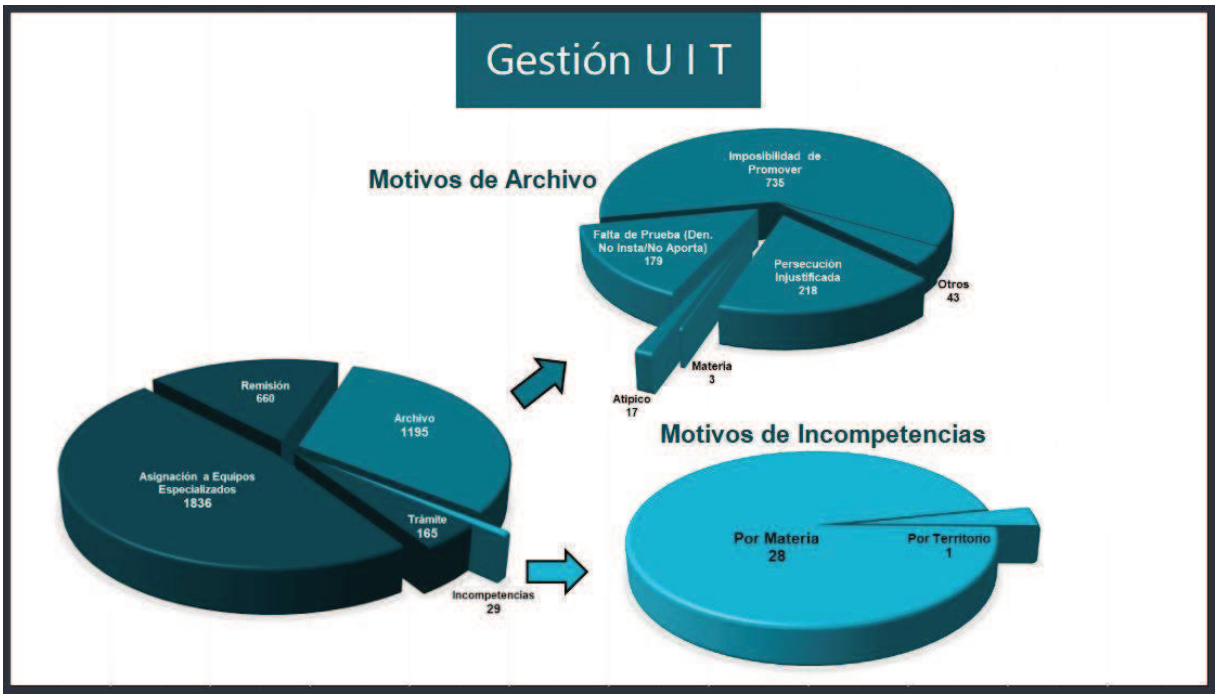
En relación a las contravenciones, se reportaron 429 casos de suplantación de identidad, 112 casos de difusión no autorizada, 1 casos de suministro de pornografía a menores y 107 casos de hostigamiento digital. Recordemos que las

[97] (El National Center for Missing & Exploited Children es una corporación privada 501(c)(3), sin ánimo de lucro cuya misión es ayudar a encontrar a los niños perdidos, reducir la explotación sexual infantil y evitar que los niños sean víctimas. El NCMEC trabaja con las familias, las víctimas, la industria privada, las fuerzas del orden y el público en general para ayudar a evitar secuestros infantiles, recuperar a los niños perdidos y brindar servicios para impedir y combatir la explotación sexual infantil.

[98] Debe tenerse en consideración el contexto que la restricción obligatoria generada por el virus COVID-19, generó un incremento extraordinario de los casos de delitos informáticos, particularmente de los casos de estafas.

contravenciones son infracciones menores o violaciones de leyes, reglamentos o normativas que no constituyen delitos graves. En este caso, considerando que la fiscalía es de Ciudad Autónoma de Buenos Aires, se considera aplicable el Código Contravencional de la Ciudad Autónoma de Buenos Aires[99].

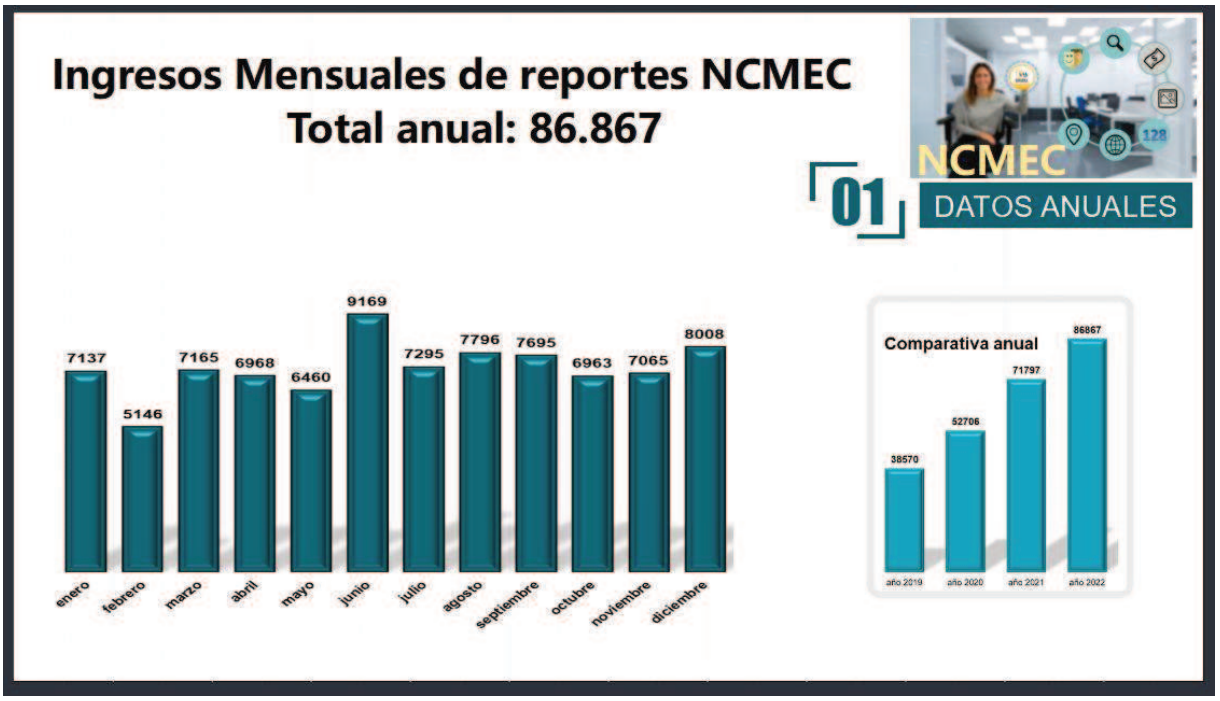
De la totalidad de casos recibidos desde la UIT (tanto de delitos como de contravenciones) la fiscalía informa que 1836 casos fueron asignados a Equipos Especializados, 660 casos han sido pasados a Remisión (suspensión del proceso penal), 1195 casos han sido archivados, 29 casos se ha declarado la incompetencia de la fiscalía y en 165 casos se ha dado trámite.



La fiscalía informa además los motivos del archivo de las causas, donde podemos observar que 735 casos han sido por imposibilidad de promover, 179 casos por falta de prueba (el denunciante no insta o no aporta), 17 casos por atipicidad, 3 casos por razón de la materia y 218 casos se ha considerado persecución injustificada. Por otra parte, se informa que de los 29 casos de incompetencia, 28 casos han sido en razón de la materia y 1 sólo caso en razón del territorio. Esta información es super

[99] Código Contravencional de la Ciudad de Buenos Aires: Url: http://www.saij.gob.ar/1472-local-ciudad-autonoma-buenos-aires-codigo-contravencional-ciudad-lpx0001472-2004-10-28/123456789-0abc-defg-274-1000xvorpyel

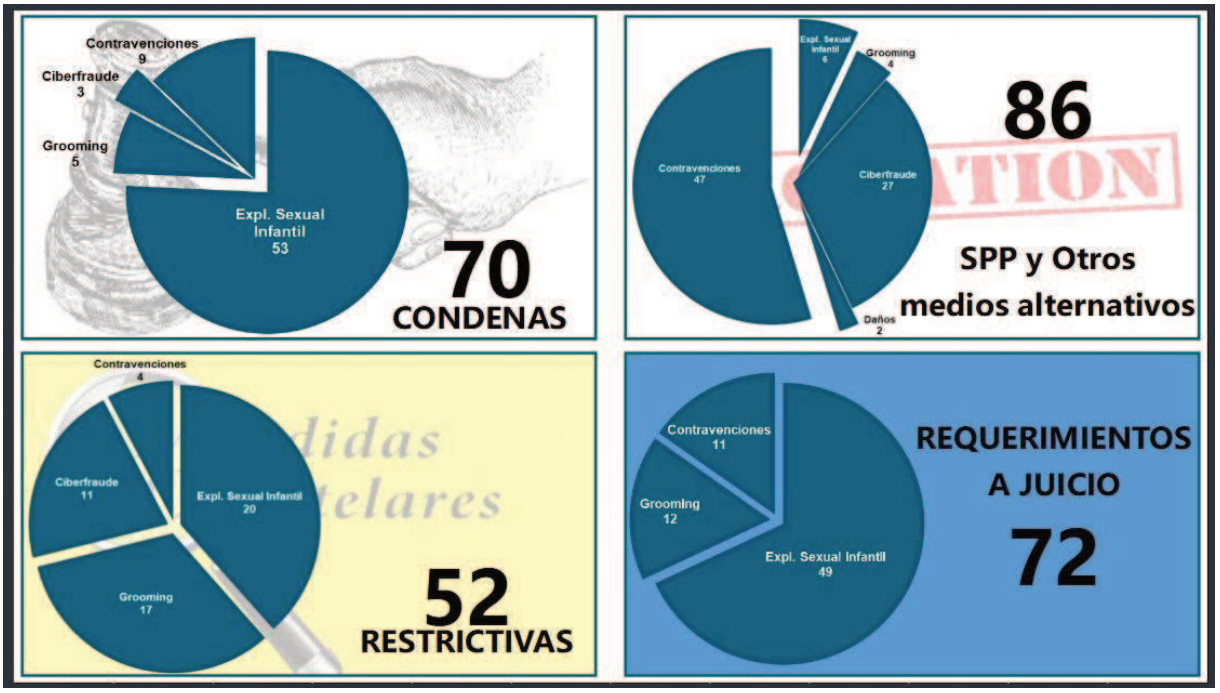
importante y celebramos que esta fiscalía brinde este nivel de detalle, que permiten conocer con rigurosidad el actual estado de situación de las denuncias.



En relación a los ingresos de causas por reportes de NCMEC, la fiscalía informa el índice de ingresos mensuales, destacando que los ingresos más altos son del mes de Junio y Diciembre.

También nos parece de interés destacar cómo se han ido incrementando anualmente los reportes NCMEC, donde entre los años 2020 y 2021 los reportes tuvieron un incremento anual del 36% anual, mientras que en el 2022 aumentó un 20% en relación a los reportes del año anterior.

Especialmente en época de pandemia, se ha observado un marcado incremento en la incidencia y sofisticación del ciberdelito, lo que ha planteado nuevos y complejos desafíos en el ámbito legal. La combinación de factores como el aumento significativo de la actividad en línea, la dependencia de las tecnologías de la información y la comunicación, así como la vulnerabilidad emocional y financiera de la población en momentos de crisis, ha creado un escenario propicio para que los actores del ciberdelito exploren oportunidades y empleen tácticas más elaboradas.



Por último, desde la Fiscalía Especializada en Delitos y Contravenciones Informáticas, dirigida por la Dra. Daniela Dupuy, nos informan que durante el año 2022 se han logrado:

- 70 condenas, de las cuales:
  - 53 son de casos de explotación sexual infantil
  - 5 por casos de grooming
  - 3 por ciberfraude
  - 9 por casos de contravenciones.
- 52 medidas restrictivas, de las cuales:
  - 20 son de casos de explotación sexual infantil
  - 17 por casos de grooming
  - 11 por ciberfraude
  - 4 por casos de contravenciones
- 86 SPP y Otros medios alternativos, de los cuales:
  - 6 son de casos de explotación sexual infantil
  - 4 por casos de grooming
  - 27 por ciberfraude
  - 47 por casos de contravenciones
  - 2 por casos de daños

- 72 requerimientos de elevación a juicio, de los cuales:
  - 49 son de casos de explotación sexual infantil
  - 12 por casos de grooming
  - 11 por casos de contravenciones

3.3.2. Muestreos oficiales del Ministerio de Justicia y Derechos Humanos de la Nación Argentina

El primer muestreo[100] se ha publicado oficialmente en Septiembre de 2016, bajo el título "Una aproximación a la estadística criminal sobre delitos informáticos: Primer muestreo de denuncias judiciales de la República Argentina – Año 2013".

En dicha publicación, se afirma: *"No se conocen antecedentes en la República Argentina de un estudio estadístico de denuncias judiciales sobre delitos informáticos a nivel nacional. En el marco de las competencias asignadas a la Dirección Nacional de Política Criminal en materia de Justicia y Legislación Penal —elaborar la estadística oficial en materia delictiva y el funcionamiento del sistema penal—[101], el objetivo de este informe es realizar una aproximación sobre qué tipo de hechos ilícitos son denunciados en los tribunales de la República Argentina que tengan vinculación directa con dispositivos informáticos, sea como medio para cometer un delito o como blanco del crimen mismo. Para tal fin, se decidió realizar una prueba piloto a modo de muestreo de presentaciones judiciales realizadas bajo figuras penales contenidas en la ley 26.388, tanto en los fueros federales como en los penales y contravencionales.*

[100] Dirección Nacional del Sistema Argentino de Información Jurídica, Secretaría de Planificación Estratégica, Ministerio de Justicia y Derechos Humanos de la Nación Argentina, "Una aproximación a la estadística criminal sobre delitos informáticos: Primer muestreo de denuncias judiciales de la República Argentina – Año 2013", Editorial: Ministerio de Justicia y Derechos Humanos de la Nación; ISBN: 978-987-4196-05-7, Publicado en Septiembre de 2016.

[101] Resolución 1451/2012, Ministerio de Justicia y Derechos Humanos de la Nación

En esta primera etapa se realizó un relevamiento estadístico de denuncias registradas en los fueros criminales y correccionales de la provincia de Buenos Aires en base estadísticas brindadas por la Procuración General de la Suprema Corte de Justicia provincial, las denuncias recibidas por Fiscalía especializada en delitos informáticos de la Ciudad Autónoma de Buenos Aires, y las causas iniciadas por los tribunales federales en todo el país de acuerdo a datos aportados por el Ministerio Público Fiscal de la Nación. En términos de uso de computadoras, de los 20.057.965 habitantes que utilizan PCs a nivel nacional[102]*, la CABA y el distrito bonaerense concentran más de la mitad de los usuarios de todo el país, con un total de 10.192.657 personas, lo que permite tener una muestra significativa en términos representativos a nivel nacional*[103]*.* Los datos brindados en este informe se corresponden con las presentaciones iniciadas en estos distritos en el período que va del 1 de enero al 31 de diciembre de 2013.

El propio informe reconoce que "*de ninguna manera el informe pretende representar una muestra acerca del fenómeno del cibercrimen en el país",* y que para la realización de un informe más integral "*el mismo debe complementarse con estudios tales como encuestas de victimización, causas tramitadas por juzgados de faltas y contravenciones que involucren dispositivos informáticos, denuncias recibidas por organismos públicos relacionados —como por ejemplo, la Dirección Nacional de Protección de Datos Personales— y reportes de incidentes de empresas de seguridad informática, entre otros."*

De lo expuesto destacamos primero el reconocimiento oficial que este estudio había adelantado sobre que "*no se conocen antecedentes en la República Argentina de un estudio estadístico de denuncias judiciales sobre delitos informáticos a nivel nacional*".

Ingresando en la información brindada por el estudio precitado, en el punto 2, "Fuero federal de la República Argentina", sobre las causas judiciales de acuerdo a

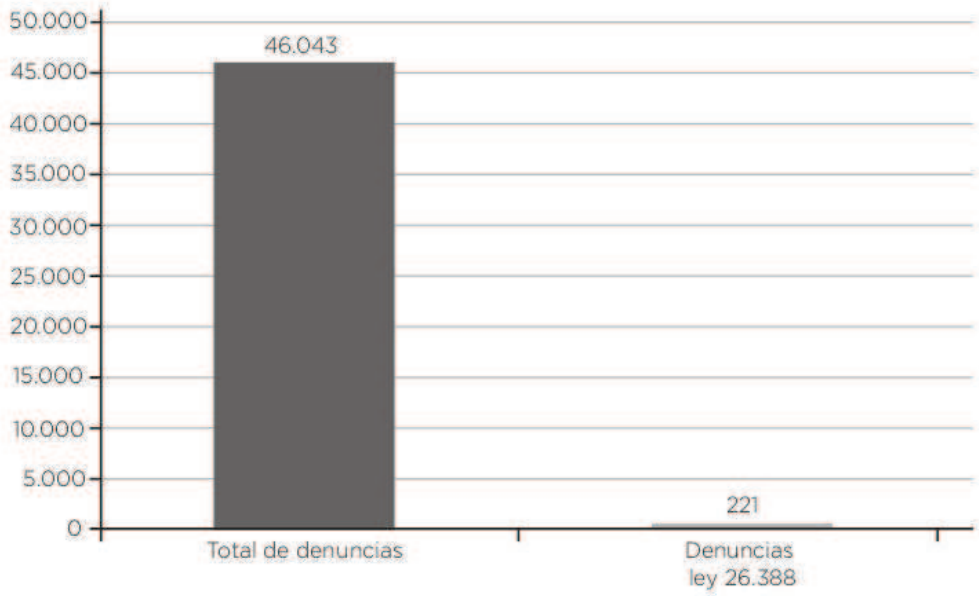
[102] La representatividad de la muestra es en base al uso de computadoras hogareñas, ya que si bien los ciudadanos acceden a la red a través de celulares inteligentes, se estableció como dato de referencia la disponibilidad de dispositivos estacionarios geográficamente.

[103] Datos según el censo 2010, Instituto Nacional de Estadísticas y Censos, Ministerio de Economía y Finanzas Públicas de la Nación.

la ley 26.388, a nivel país en el año 2013, se exhibe que según datos del Ministerio Público Fiscal de la Nación, de un total de 46.043 causas judiciales que tramitó el fuero federal en todo el país, 221 involucraron alguna de las figuras penales de la ley 26.388, lo que representa el 0,48% del total de casos registrados durante 2013.

Esto significa que, de cada 200 delitos denunciados, uno se encuentra bajo alguna figura penal de la ley de delitos informáticos, lo que demuestra su bajo nivel en comparación con el resto de las presentaciones realizadas.

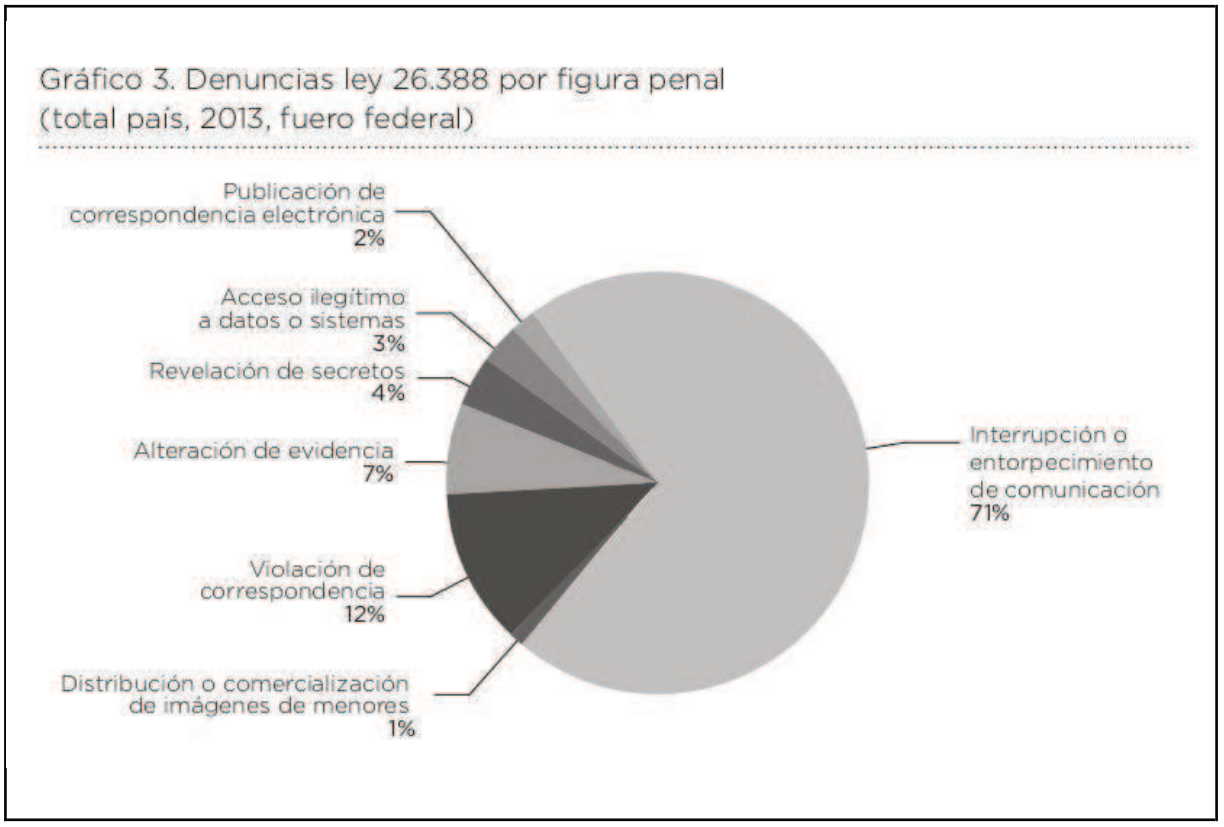
Gráfico 1. Total denuncias/denuncias ley 26.388 (total país, 2013, fuero federal)



Por otro lado, se informa (Gráfico 3) que la mayoría de las denuncias federales —7 de cada 10— corresponden a la figura de interrupción o entorpecimiento de comunicaciones, con 158 causas iniciadas por sobre un total de 221 presentaciones durante 2013.

La figura que le sigue en cantidad de presentaciones es la violación de correspondencia electrónica, con 26 causas, lo que representa un 12% del total de casos. En tercer y cuarto lugar aparecen las figuras de alteración de evidencia

informática con 16 denuncias —7%—, y la revelación de documentos secretos por parte de un funcionario público, con 8 casos —4%—. En tanto que ambas figuras pueden estar relacionadas con el desarrollo de una causa judicial si la revelación de información secreta supone la incriminación de alguna persona en términos penales. Entre ambas figuras suman un 11% del total —24 casos—. En cuanto al ofrecimiento y distribución de imágenes de menores de edad desnudos o representación de los mismos, solo 3 denuncias fueron administradas por la justicia federal, lo que representa un 1% del total de causas durante el año en cuestión.

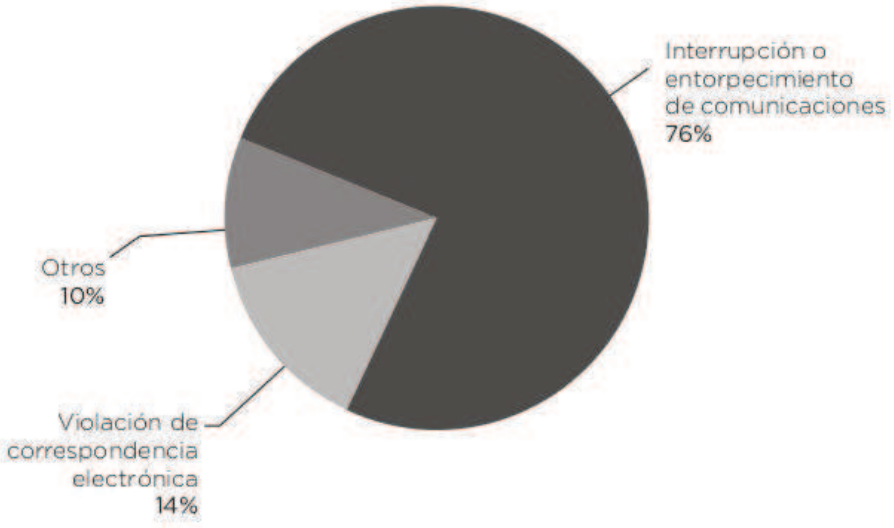


Para completar la cita, traeremos también las estadísticas recolectadas sobre delitos informáticos en el 2013 en la Ciudad Autónoma de Buenos Aires:

Figura penal	Denuncias
Art. 197 CP: Interrupción o entorpecimiento de comunicaciones	64
Art. 153 CP: Violación de correspondencia electrónica	12
Art. 255 CP: Alteración de evidencia informática	3
Art. 153 bis CP: Acceso ilegítimo a sistema o dato informático	2
Art. 155 CP: Publicación indebida de comunicaciones	1
Art. 128 CP: Distribución o comercialización de imágenes de menores	1
Art. 157 CP: Revelación de secretos	1
Total	84

Fuente: Ministerio Público Fiscal de la Nación.

Gráfico 4. Denuncias ley 26.388 por figura penal (CABA, 2013, fuero federal)



Al igual que en los datos del total país, la mayoría de las denuncias recibidas en la ciudad de Buenos Aires corresponden al delito de interrupción o entorpecimiento de comunicaciones, con un promedio mayor a la media nacional —76%—. Con 64 denuncias recibidas por sobre un total de 84, 3 de cada 4 causas iniciadas en ese distrito pertenecen a esta figura. La segunda figura en importancia

es la violación de correspondencia electrónica, con un total de 12 denuncias, lo que representa un 14% del total general de causas.

No replicaremos aquí todo el trabajo realizado, por lo cuál remitimos al lector a su acceso[104] y reproduciremos los aspectos más relevantes -a nuestro criterio- de las conclusiones alcanzadas.

Entre sus conclusiones finales, el trabajo afirma que tras la realización de esta primer prueba piloto sobre causas tramitadas en base a las figuras de la ley 26.388 en los fueros en cuestión y el bajo nivel de causas tramitada por los tribunales de los distritos que fueron parte del muestreo, se pueden trazar algunas hipótesis sobre la base de los datos disponibles, tanto así como interrogantes que podrán marcar algunos lineamientos para estudios futuros, tanto a nivel estadístico como de tipo cualitativo.

Como primera conclusión se puede afirmar que, como sucede en otras partes del mundo, los delitos que involucran dispositivos informáticos poseen un bajo nivel de denuncia en los tribunales de la República Argentina[105].

De los porcentajes analizados, el fuero federal demuestra un porcentaje mayor de causas relacionadas con delitos informáticos que el fuero criminal y correccional en comparación con el total general de causas tramitadas en el período en cuestión —0,48% del total de denuncias iniciadas por el Ministerio Público Fiscal de la Nación a nivel país y 0,04 en los tribunales de la provincia de Buenos Aires—. Esto podría deberse a que cuando mayor nivel de complejidad y/o gravedad en cuanto al tipo de delito denunciado, mayor nivel de denuncia.

Esto parece demostrarse con la mayor cantidad de denuncias recibidas en todo el territorio en los tribunales federales sobre el delito de interrupción o entorpecimiento de comunicaciones, que si bien el art. 197 CP refiere a todo tipo comunicaciones —no solo a las mediadas por dispositivos informáticos, sino también

[104] Dirección Nacional del Sistema Argentino de Información Jurídica, Secretaría de Planificación Estratégica, Ministerio de Justicia y Derechos Humanos de la Nación Argentina, "Una aproximación a la estadística criminal sobre delitos informáticos: Primer muestreo de denuncias judiciales de la República Argentina – Año 2013", Editorial: Ministerio de Justicia y Derechos Humanos de la Nación; ISBN: 978-987-4196-05-7, Publicado en Septiembre de 2016.

[105] La negrita pertenece al autor, y se destaca a fin de señalar dicha frase como un reconocimiento oficial de la existencia de una importante cifra negra en delitos informáticos en Argentina.

telegráficas y telefónicas— alude a la imposibilidad de funcionamiento de los sistemas en sí. En los casos de comunicaciones digitales, dicha figura puede incluir la caída del servicio de Internet a usuarios particulares u organizaciones, el "hackeo" de redes informáticas o cualquier servicio de Internet en términos de acceso o comunicación, entre otros.

En términos criminológicos, algunos delitos son más denunciados que otros en función de la proporcionalidad a la ofensa que produce en ciertos sectores de la sociedad. Esto parece demostrarse en términos por el importante volumen de presentaciones judiciales relacionadas con el ofrecimiento y distribución de material relacionado con menores de edad desnudos o representaciones de los mismos por medios informáticos. En la ciudad de Buenos Aires la mayoría de las denuncias recibidas por la fiscalía especializada refieren a esta figura, tanto así como en la provincia de Buenos Aires, que ocupan más de un tercio de las causas iniciadas.

Esto evidencia la preocupación y sensibilidad de la ciudadanía para esclarecer y perseguir penalmente a los responsables de delitos que ponen en riesgo la integridad de los menores de edad, en esta oportunidad ante posibles casos de acoso sexual o pedofilia, sea mediante la obtención de imágenes de menores desnudos por medio de webcam o la descarga o intercambio de material de abuso sexual infantil a una computadora, entre otras.

Otra conclusión a la que se puede arribar es que la cantidad de usuarios de computadoras por región tampoco resulta ser una variable ni un factor condicionante para explicar un caudal de denuncias de delitos de tipo informáticos. Tanto a nivel de denuncias federales como de justicia ordinaria, los datos estadísticos entre cantidad de delitos por habitante y porcentaje de personas que utilizan computadoras por regiones no establecen una correlación directa. Independientemente de esta afirmación, cabe destacar que en todo el territorio nacional existe un porcentaje similar de usuarios de computadora, sin demasiadas variables significativas entre regiones.

Por último, cabe señalar a modo de cierre la importancia que parece adquirir la privacidad y la intimidad de las personas como usuarios de Internet, sobre todo si se tiene en cuenta que hubo un una cantidad significativa de presentaciones judiciales relacionadas con las figuras penales de acceso ilegítimo a sistema o dato

informático, violación de correspondencia electrónica y del art. 157 bis CP, alusivo a delitos relacionados con la protección de los datos personales. Si bien representan un porcentaje menor en cuanto a otras figuras antes señaladas, que existan denuncias sobre estos tipos de delitos demuestra la importancia de la privacidad y la intimidad de las comunicaciones en línea para los ciudadanos.

El segundo muestreo[106] fue publicado oficialmente en Mayo de 2017 bajo el título "Estudios estadísticos sobre cibercrimen: Segundo muestreo de denuncias judiciales de la República Argentina Año 2014", dirigido por Gustavo Sain.

Nuevamente, tal como sucedió del análisis del primer muestreo, desde el comienzo del nuevo estudio se afirma que "*Como se señaló en el informe "Primer muestreo de denuncias judiciales de la República Argentina. Año 2013", (Ministerio de Justicia y Derechos Humanos de la Nación, 2016) el análisis de los resultados de los diferentes estudios estadísticos sobre este tipo de conductas no refleja el estado de situación acerca del nivel de cibercrimen en un determinado país o región, en tanto que muchas de las conductas ilícitas e ilegales que involucran dispositivos informáticos no se denuncian en los tribunales de justicia. Si bien todo registro estadístico sobre hechos de violencia e inseguridad posee una cifra oculta por diferentes factores, los llamados "delitos informáticos" son denunciados en la justicia en un ínfimo porcentaje.*

Para Lucía Dammert, Felipe Ruz y Felipe Zalazar*, "los registros delictuales de la política no representan fielmente la tasa de delitos ocurridos en un determinado territorio durante un período específico, dado que indican aquellos delitos que han sido denunciados y registrados por la institución" (Dammert, Ruz & Zalazar, 2008). Asimismo, los autores señalan para el caso de la estadística general de delitos que también se deben tener en cuenta las diferentes motivaciones que tiene la ciudadanía para realizar una denuncia acerca de un delito que haya afectado un bien o a su persona. En este sentido señalan que "está mediado por factores como el grado de confianza en la fuerza pública y el sistema de justicia en general, el tipo*

[106] Dirección Nacional de Política Criminal en materia de Justicia y Legislación Penal, Secretaría de Justicia, Ministerio de Justicia y Derechos Humanos de la Nación Argentina, "Segundo muestreo de denuncias judiciales de la República Argentina : Año 2014" / Gustavo Sain. - 1a ed . - ISBN: 978-987-4196-06-4; Ciudad Autónoma de Buenos Aires : Ediciones SAIJ, Publicado en Mayo 2017

de delito del que ha sido víctima y la inexistencia de incentivos externos para realizarla".

A párrafo siguiente, se realiza un breve pero preciso análisis sobre las causas o factores que pueden dar explicación a la gran cantidad de delitos informáticos no denunciados: "*Para el caso de los ciberdelitos, el grado de confianza en la fuerza pública y el sistema de justicia se encuentra dado por un porcentaje significativo de la población que percibe la imposibilidad de resolución de este tipo de conductas por la falta de indicios acerca de los verdaderos responsables de determinados delitos. Algunos factores que explican esto son: el anonimato que ofrece Internet a partir de la posibilidad de construir identidades ficticias en la nube, el hecho de que muchos de los responsables de este tipo de ilícitos se encuentran en otros países, la falta de capacitación y formación de los agentes responsables de la investigación y la ausencia de herramientas técnicas y legales para abordar las investigaciones, entre otros.*

De esta introducción podemos extraer varios elementos de destacada relevancia para el presente trabajo. En principio, afirmar nuevamente y de forma quizás más explícita, el reconocimiento del problema de la cifra negra como motivador del muestreo en sí, y a su vez, de esta tesis de doctorado.

En segundo lugar, destacar que se menciona entre las causas fundamentales de la no denuncia, a la falta de confianza en la fuerza pública y el sistema de justicia. Dicha falta de confianza, a su vez, es explicada por el estudio por diferentes elementos que a continuación identificamos:

1. Anonimato;
2. Transnacionalidad;
3. Falta de capacitación y formación de los agentes responsables de la investigación;
4. Ausencia de herramientas técnicas y legales para abordar las investigaciones.

En relación al alcance de este segundo muestreo, en esta segunda etapa, y al igual que en el primero de ellos, se realizó un relevamiento estadístico de denuncias registradas en los fueros criminales y correccionales de la provincia de Buenos Aires en base a la estadística brindada por la Procuración General de la Suprema Corte de Justicia, las presentaciones recibidas por la fiscalía especializada en delitos

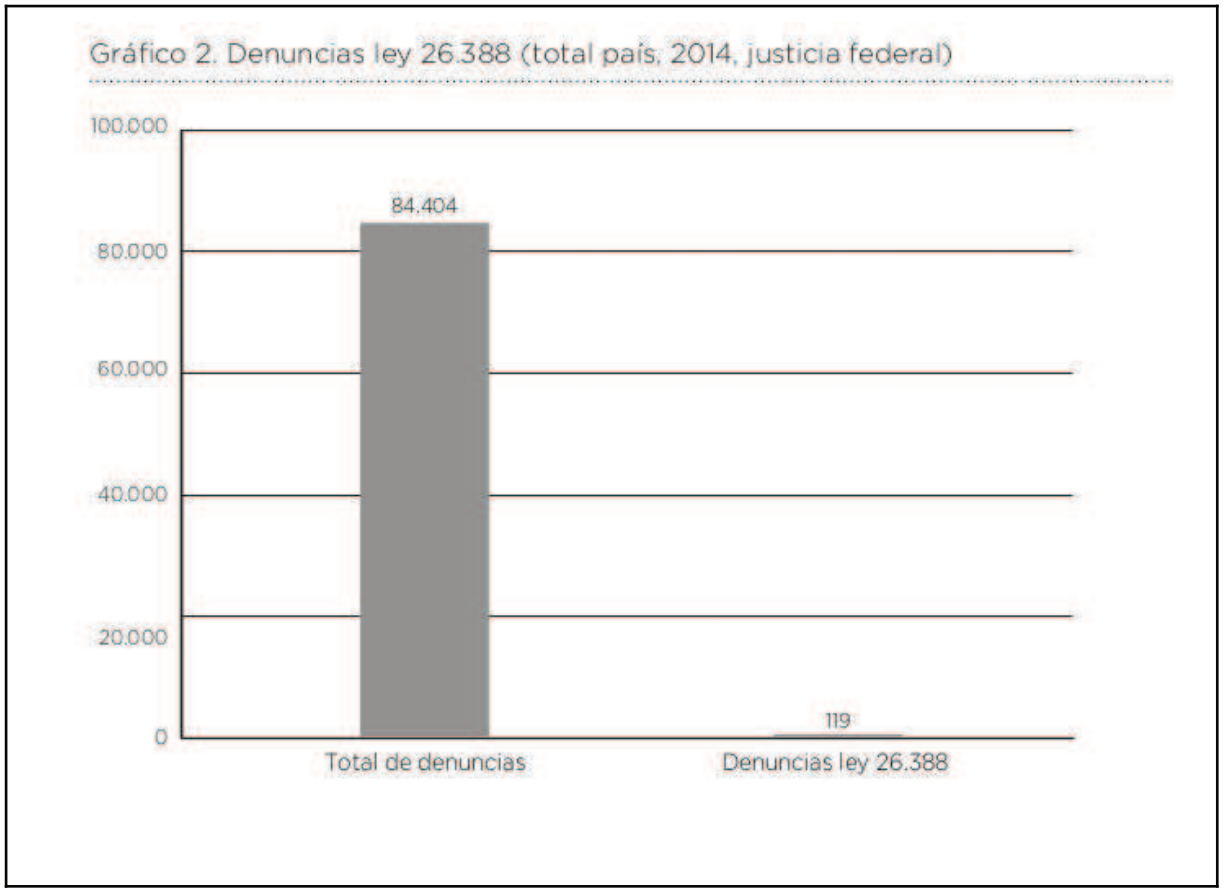
informáticos de la Ciudad Autónoma de Buenos Aires y las causas iniciadas por los tribunales federales en todo el país de acuerdo a datos aportados por el Ministerio Público Fiscal de la Nación.

En esta oportunidad se incorpora a la estadística la figura de grooming o acoso sexual por parte de un adulto a través de servicios y aplicaciones de Internet. Mediante la aprobación de la ley 26.904, en noviembre de 2013, se incorporó al Código Penal de la Nación el art. 131 que penaliza esta modalidad de acoso virtual.

Antes de la promulgación de dicha norma, la mayoría de estos hechos eran encuadrados dentro del art. 128 CP, fundamentalmente en aquellos casos donde la víctima era inducida a desnudarse frente a la webcam o el acosador enviaba material fotográfico por medios electrónicos como medio de atracción.

Asimismo, también se incorporan datos estadísticos de la provincia de Santa Fe, a partir de los datos brindados por el Ministerio Público de la Acusación, tanto como estadísticas de denuncias recibidas por el Equipo Niñ@s del Programa "Las víctimas contra las violencias" del Ministerio de Justicia y Derechos Humanos de la Nación en tanto organismo nacional competente en la recepción de denuncias relacionadas con grooming, violencia contra niñas, niños y adolescentes en Internet y pornografía infantil.

Al igual que la primer muestra, se afirma que "*la finalidad del presente informe es la de tener una aproximación sobre aquellas conductas delictivas que involucran dispositivos informáticos que llegan al ámbito de la justicia, es decir, qué delitos informáticos se denuncian en los tribunales de los distritos que componen la muestra, y que de ninguna manera pretende representar una muestra acerca del fenómeno del cibercrimen en el país*".



Con respecto a los datos expuestos, en el fuero federal se registró una disminución del 46% en relación al año anterior, donde de un total de 221 casos denunciados en 2013 se registraron 102 casos menos.

Esto no se debe a una baja en la cantidad de denuncias ingresadas sino a que los datos reportados por el Ministerio Público Fiscal de la Nación durante el año 2013 incluían las denuncias tramitadas por los tribunales nacionales de Capital Federal, en la actualidad en proceso de transferencia a la órbita jurisdiccional de la Ciudad Autónoma de Buenos Aires.

Tabla 1. Denuncias ley 26.388 por distrito (total país, 2014)

Distrito	Denuncias
CABA	67
Provincia de Buenos Aires	23
Salta	4
Santa Fe	3
Mendoza	3
Río Negro	3
Córdoba	2
Entre Ríos	2
Chaco	2
Jujuy	2
San Juan	2
Tucumán	2
Chubut	1
Formosa	1
La Pampa	1
Santiago del Estero	1
TOTAL	119

En la tabla 1 podemos observar que la mayoría de las denuncias presentadas en los tribunales federales se iniciaron en la Ciudad Autónoma de Buenos Aires, con un total de 67 denuncias sobre 119. Si bien representa una cantidad menor de presentaciones que el año anterior —84 causas en 2013—, incrementó su porcentaje en relación al total de denuncias en todo el territorio. En este sentido, más de la mitad de las causas tramitadas en 2014 se iniciaron en ese distrito con un 56% del total contra 38% del período anterior.

El segundo distrito con mayor cantidad de causas es la provincia de Buenos Aires, con 23 denuncias, casi la mitad de denuncias tramitadas por CABA en el período en cuestión, con 19% del total de denuncias recibidas. Si se suma la cantidad de denuncias entre PBA y CABA, ambas concentran el 75% de

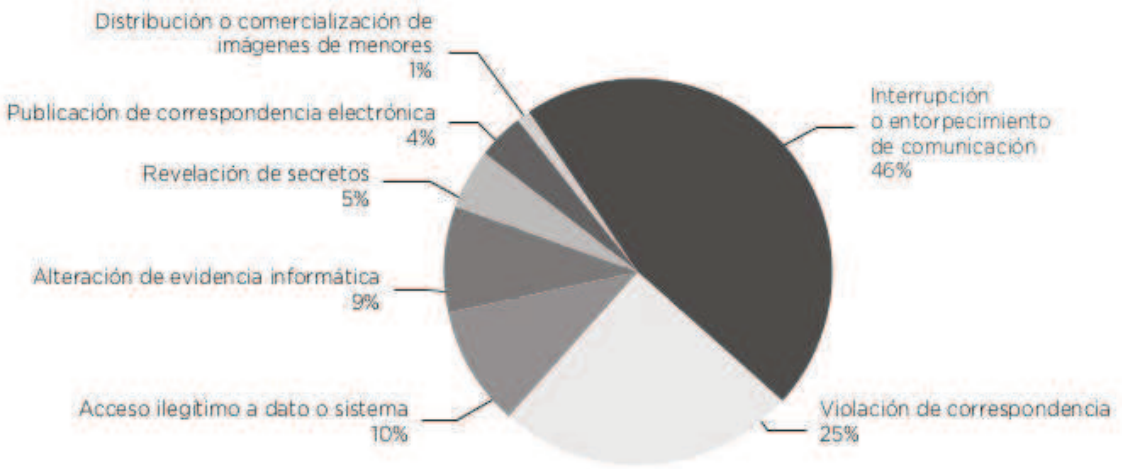
presentaciones, lo que representa tres de cada cuatro denuncias relacionadas con figuras penales de la ley 26.388 en todo el territorio nacional. El resto de los distritos se distribuyen equitativamente el porcentaje de causas tramitadas a nivel federal con no más del 5% de causas en relación al total. El tercer distrito en la escala es la Provincia de Salta con cuatro presentaciones, seguidas por Santa Fe, Mendoza y Río Negro, con tres cada una.

Tabla 3. Denuncias leyes 26.388 y 26.904 por figura penal (total país, 2014)

Figura penal	Denuncias
Art. 197 CP: interrupción o entorpecimiento de comunicaciones	54
Art. 153 CP: violación de correspondencia electrónica	30
Art. 153 bis CP: acceso ilegítimo a sistema o dato informático	12
Art. 255 CP: alteración de evidencia informática	11
Art. 157 CP: revelación de secretos	6
Art. 155 CP: publicación indebida de comunicaciones	5
Art. 128 CP: distribución o comercialización de imágenes de menores	1
TOTAL	119

Fuente: Ministerio Público Fiscal de la Nación.

Gráfico 6. Denuncias leyes 26.388 y 26.904 por figura penal (total país, 2014)

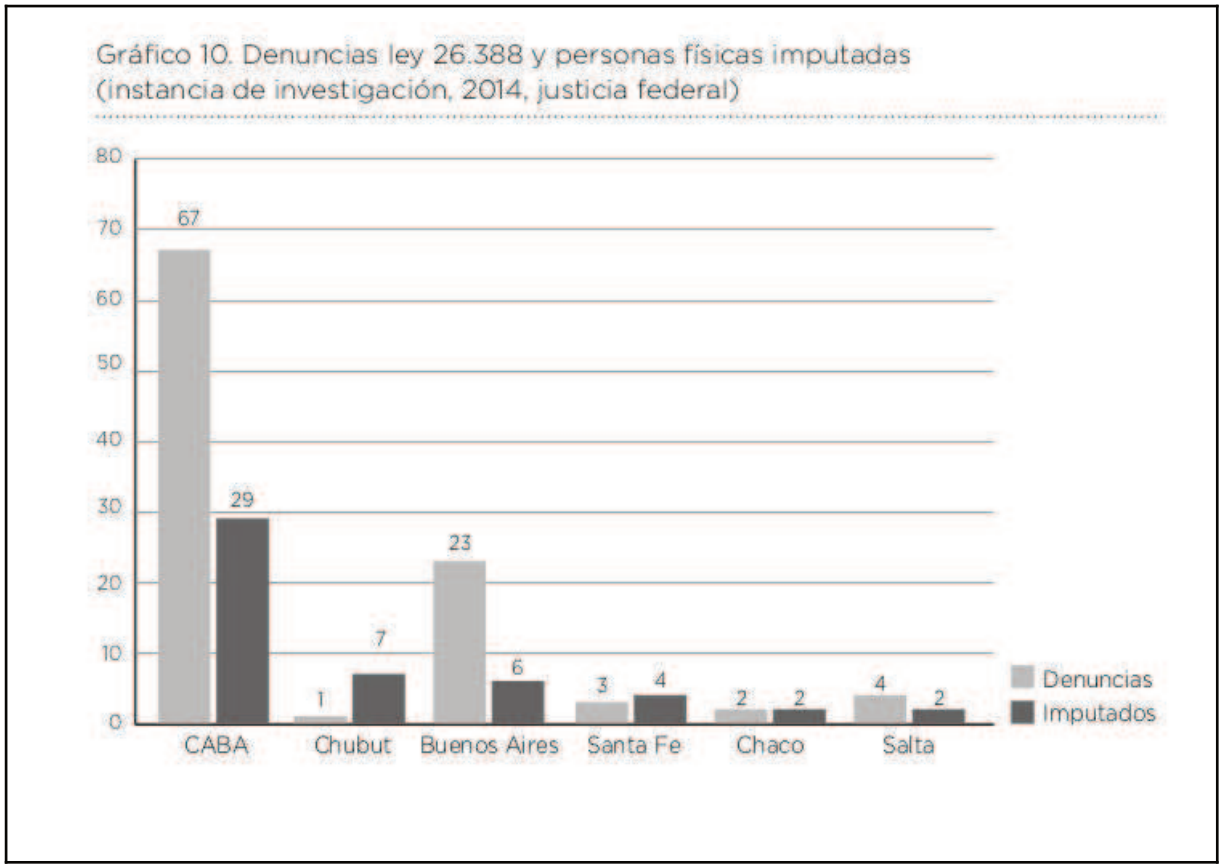


En la tabla 3, puede observarse el análisis realizado categorizado por denuncias por figura penal. Si se discrimina el total de las denuncias por figura penal de las leyes 26.388 y 26.902 los resultados son los siguientes:

Al igual que el año anterior, la mayor cantidad de denuncias judiciales se encuadran bajo la figura de interrupción o entorpecimiento de comunicaciones con casi la mitad de causas iniciadas —54 presentaciones sobre 119 en total—. En 2013, siete de cada diez denuncias —71%— estaban relacionadas con esta figura, lo que demuestra una disminución en su porcentaje (Ministerio de Justicia y Derechos Humanos de la Nación, 2016).

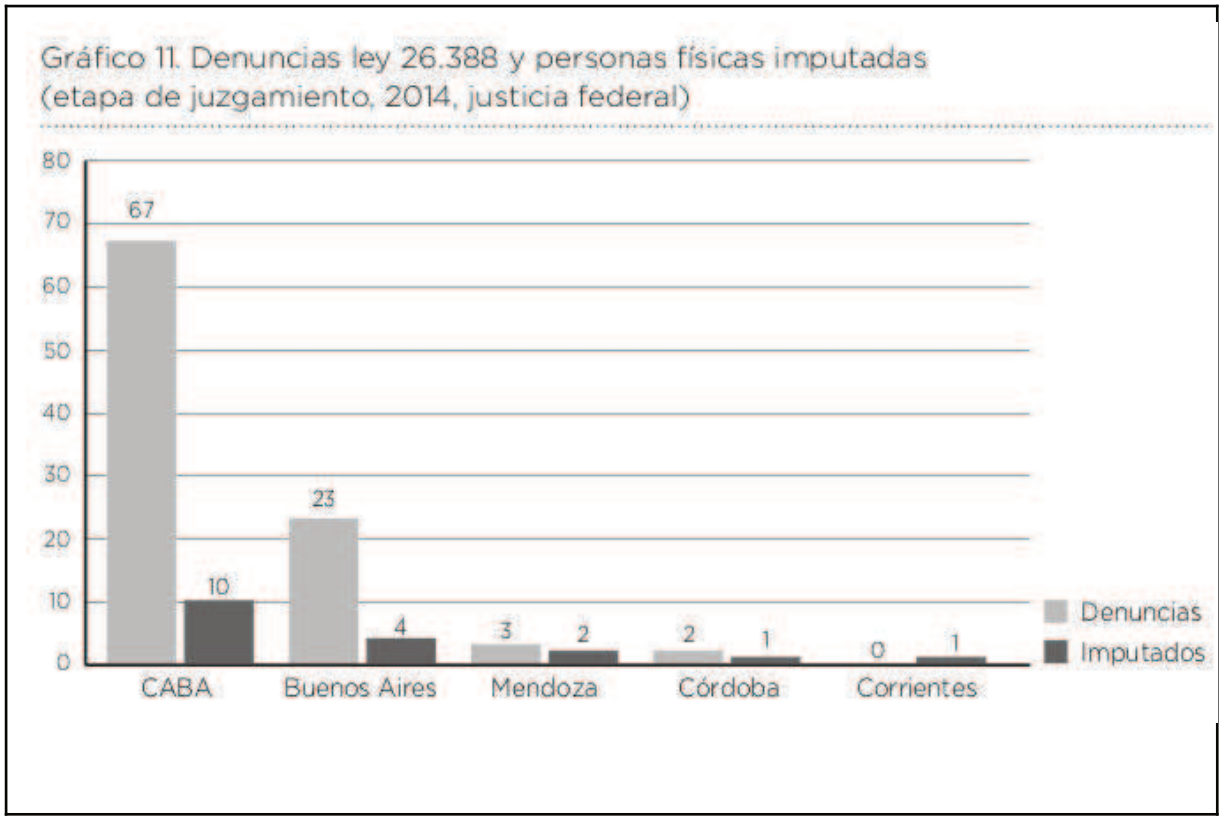
La segunda figura sigue siendo la violación de correspondencia electrónica. Durante 2014, una de cada cuatro causas se relacionan con esta figura —el 25% de denuncias sobre el total—, mientras que en 2013 solo el 12% de las mismas se enmarcaban bajo la misma. Una de cada 10 denuncias se engloba bajo el acceso ilegítimo a dato o sistema informático, con 12 causas relacionadas.

Como datos adicionales -a comparación del primer muestreo- en esta segunda versión 2014, se ha realizado una profundización sobre la situación procesal de las denuncias recolectadas.

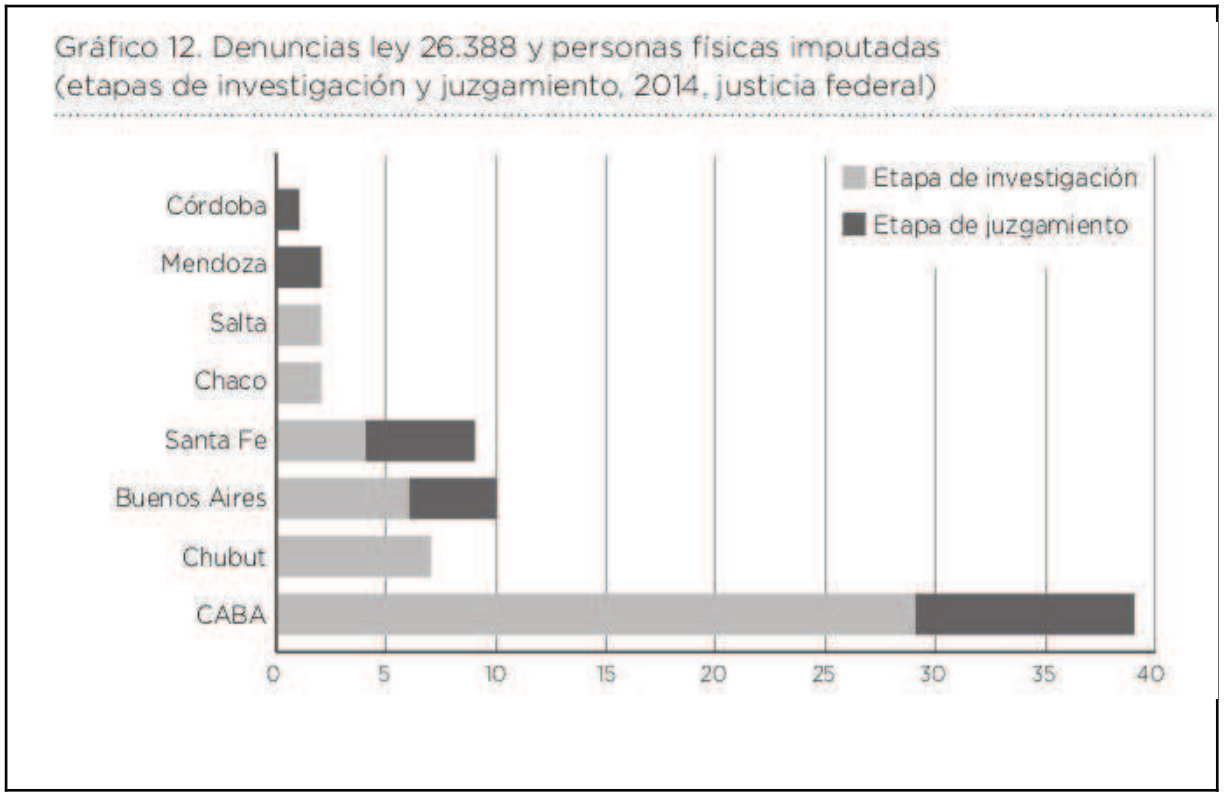


En la etapa de investigación, de 100 denuncias se imputaron a 50 personas, siendo las mismas personas físicas en su totalidad, lo que arroja un promedio de una persona imputada cada dos causas.

El distrito con mayor cantidad de imputados es la Ciudad Autónoma de Buenos Aires con 29 personas físicas en 67 causas, lo que implica un promedio de 0,43 personas por causa. Le sigue la provincia de Chubut, que pese a tener una sola causa en curso, registra siete personas imputadas. Junto con Santa Fe —cuatro imputados en tres causas— son los únicos dos distritos que poseen más de un imputado por causa en esta instancia. La provincia de Buenos Aires es el distrito con menor porcentaje de imputados, con seis personas físicas en 23 causas en curso durante el año 2014 —0,26 imputados por causa—.



En la etapa de juzgamiento la cantidad de imputados disminuye en comparación con la etapa de instrucción, de 100 denuncias existen 18 en total, todas personas físicas. En la Ciudad Autónoma de Buenos Aires la disminución entre la etapa de instrucción y juzgamiento va de 29 a 10 personas físicas, mientras que en la Provincia de Buenos Aires solo de seis a cinco imputados. Según los datos reportados, la Provincia de Corrientes tiene un imputado en esta etapa, sin denuncias relacionadas con la "Ley de delitos informáticos" durante 2014, lo que presupone que la denuncia fue realizada años anteriores.



Finalmente, citamos el gráfico 12, donde se exhibe una comparación sobre las causas en las etapas de investigación y juzgamiento, útil para comprender con mejor precisión los datos ilustrados en el muestreo.

Al igual que sostuvimos sobre el primer muestreo, sólo se ha citado en este trabajo los datos que a nuestro criterio aparecen como más relevantes, por lo cuál remitimos a acceder a su lectura[107] para observar los datos completos.

Entre las conclusiones finales, se pueden trazar algunas hipótesis sobre la base de los datos disponibles, tanto así como interrogantes que podrán marcar algunos lineamientos para estudios futuros, tanto a nivel estadístico como de tipo cualitativo.

A modo de conclusiones de este segundo estudio 2014, se reitera que tal como se señaló en el muestreo del año 2013 y en concordancia con la tendencia global,

[107] Dirección Nacional de Política Criminal en materia de Justicia y Legislación Penal, Secretaría de Justicia, Ministerio de Justicia y Derechos Humanos de la Nación Argentina, "Segundo muestreo de denuncias judiciales de la República Argentina : Año 2014" / Gustavo Sain. - 1a ed . - ISBN: 978-987-4196-06-4; Ciudad Autónoma de Buenos Aires : Ediciones SAIJ, Publicado en Mayo 2017

los datos arrojados por este relevamiento corroboraron que los delitos informáticos poseen un bajo nivel de denuncia en los tribunales de la República Argentina.

Si bien es cierto que por definición un ilícito que involucra como medio o como blanco del delito un dispositivo informático puede estar caratulada por una figura que no se encuentre bajo la ley 26.388, la mayoría de los crímenes de este tipo posee una amplia cifra oculta por los factores mencionados en el informe anterior. En cuanto a la justicia federal, el 0,14% de los delitos están relacionados con la ley nombrada, mientras que la justicia ordinaria de la Provincia de Buenos Aires representa el 0,034% del total de denuncias recibidas durante 2014.

En cuanto a los tipos de delitos mayormente denunciados tanto a nivel de justicia federal como ordinaria, en el caso de la primera la figura de interrupción o entorpecimiento de comunicaciones sigue siendo la que mayor cantidad de denuncias recibe en todo el país. Si bien el art. 197 del Código refiere a todo tipo comunicaciones —no solo las mediadas por dispositivos informáticos sino también telegráficas y telefónicas—, alude a la imposibilidad de funcionamiento de los sistemas en sí. En el caso de la justicia ordinaria, tanto en la Ciudad Autónoma de Buenos Aires como en la provincia de Buenos Aires, la mayor cantidad de presentaciones se relacionan con el art. 128 CP, es decir, el ofrecimiento y distribución de material relacionado con menores de edad desnudos o representaciones de los mismos por medios informáticos.

Respecto a los hechos denunciados en la provincia de Buenos Aires, al igual que el año 2013 la figura de alteración de evidencia informática representa un porcentaje significativo de denuncias en el distrito bonaerense, fundamentalmente en las departamentales judiciales de Lomas de Zamora y Mar del Plata. Si bien en el relevamiento anterior se planteó como hipótesis un posible aumento de hechos ilícitos tendientes a evitar el cumplimiento de una pena judicial o la resolución de un hecho mediante la eliminación de elementos probatorios, la causa podría haberse debido a la falta de personal capacitado, técnicas y/o herramientas adecuadas para llevar adelante la investigación criminal de delitos que involucran dispositivos informáticos a nivel provincial.

En relación a ello y ante el alto porcentaje de denuncias de este tipo, la Suprema Corte de Justicia de la provincia firmó un convenio con el Laboratorio de

Investigación y Desarrollo de Tecnología en Informática Forense de la Universidad FASTA de Mar del Plata para la realización de pericias relacionadas con el procesamiento de dispositivos automatizados que procesen datos e información digital a nivel provincial (Universidad FASTA, 2016).

En términos de cantidad de imputados, a nivel de justicia ordinaria la mayoría de las causas relacionadas con delitos informáticos poseen una persona física imputada, mientras que para el caso de los delitos federales, existe una imputada cada dos causas en primera instancia (igual que el año anterior).

En cuanto a los tiempos procesales, más de la mitad de las denuncias relacionadas con la ley 26.388 tanto a nivel a nivel federal como de justicia ordinaria —en este último caso tomando los datos brindados por la Ciudad Autónoma de Buenos Aires— se encuentran en trámite, mientras que aproximadamente una de cada tres se archivan por diferentes motivos.

Esto permite concluir que la resolución de las causas vinculadas con delitos conlleva un período mayor a un año de resolución, en tanto que una vez realizadas las denuncias casi la totalidad de las mismas no obtienen condena firme en un periodo menor a los 12 meses; solo existió una condena durante el año 2014 en CABA bajo la figura del art. 128 del Código Penal de la Nación.

El tercer muestreo[108] fue publicado oficialmente en Abril de 2018 bajo el título "Estudios estadísticos sobre cibercrimen: Tercer muestreo de denuncias judiciales de la República Argentina Año 2015", dirigido por Gustavo Sain.

Teniendo la misma dinámica que los muestreos anteriores y buscando destacar sólo los datos que son de interés para nuestra presente tesis, destacaremos los resultados obtenidos en el mismo en el fuero federal, dejando excluidos los datos aportados sobre la situación específica en Ciudad Autónoma de Buenos Aires y en las demás provincias.

En relación al alcance de este tercer muestreo, y al igual que en los anteriores, se realizó un relevamiento estadístico de denuncias registradas en los fueros

[108] Dirección Nacional de Política Criminal en materia de Justicia y Legislación Penal, Secretaría de Justicia, Ministerio de Justicia y Derechos Humanos de la Nación Argentina, "Tercer muestreo de denuncias judiciales de la República Argentina : Año 2015" / Gustavo Sain. - 1a ed . - Archivo Digital: descarga y online ISBN 978-987-4196-32-3; Ciudad Autónoma de Buenos Aires : Ediciones SAIJ, Publicado en Abril 2018

criminales y correccionales de la provincia de Buenos Aires en base a la estadística brindada por la Procuración General de la Suprema Corte de Justicia, las presentaciones recibidas por la fiscalía especializada en delitos informáticos de la Ciudad Autónoma de Buenos Aires y las causas iniciadas por los tribunales federales en todo el país de acuerdo a datos aportados por el Ministerio Público Fiscal de la Nación.

Gráfico 2. Denuncias ley 26.388 (total país, 2013 a 2015, justicia federal)

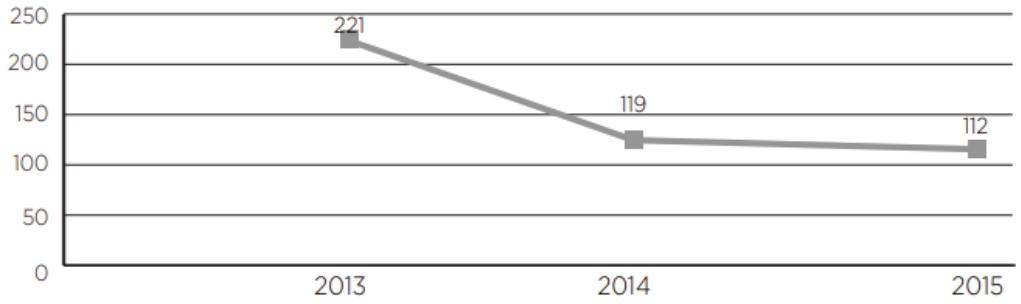
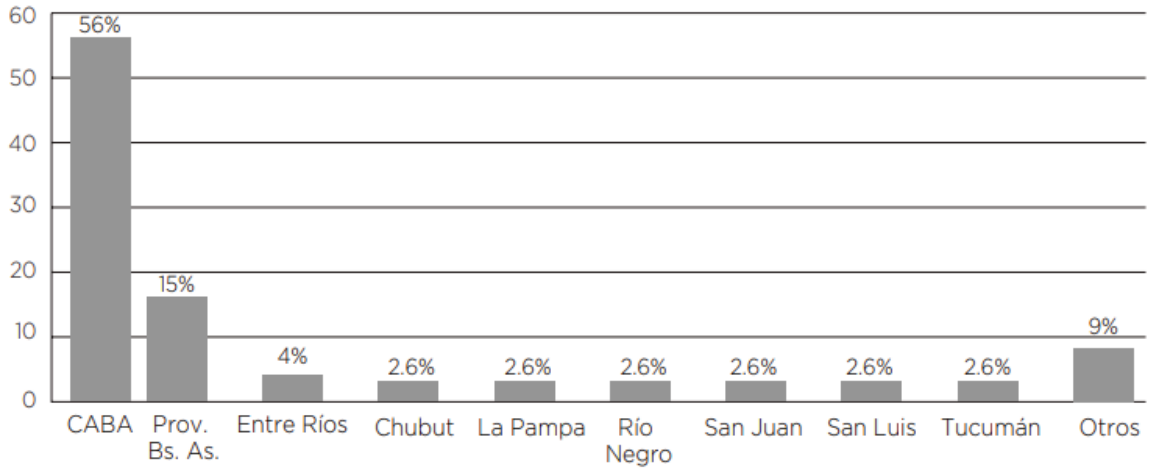


Gráfico 3. Denuncias ley 26.388 por distrito (total país, 2015, justicia federal)



De los gráficos extraídos, puede observarse que por tercer año consecutivo, la mayor cantidad de ingresos de causas vinculadas a figuras de la ley 26.388 se iniciaron en la Ciudad Autónoma de Buenos Aires, con un total de 63 denuncias sobre 112 –4 menos que el 2014–. En términos de porcentajes, representa el mismo que el año anterior –56%–, motivo por el cual más de la mitad de las denuncias federales se registran en la capital del país.

El segundo distrito con mayor cantidad de denuncias sigue siendo la Provincia de Buenos Aires con 17 presentaciones, un 15% del total. Si se suman las causas con las de la Ciudad de Buenos Aires, 8 de cada 10 denuncias se concentran en estas dos jurisdicciones. El 15% restante de denuncias se distribuyen en forma equitativa en 14 provincias, siendo la provincia de Entre Ríos la tercera jurisdicción con 4 causas –4% del total–. El resto poseen entre 3 y 1 ingreso anual por este tipo de criminalidad.

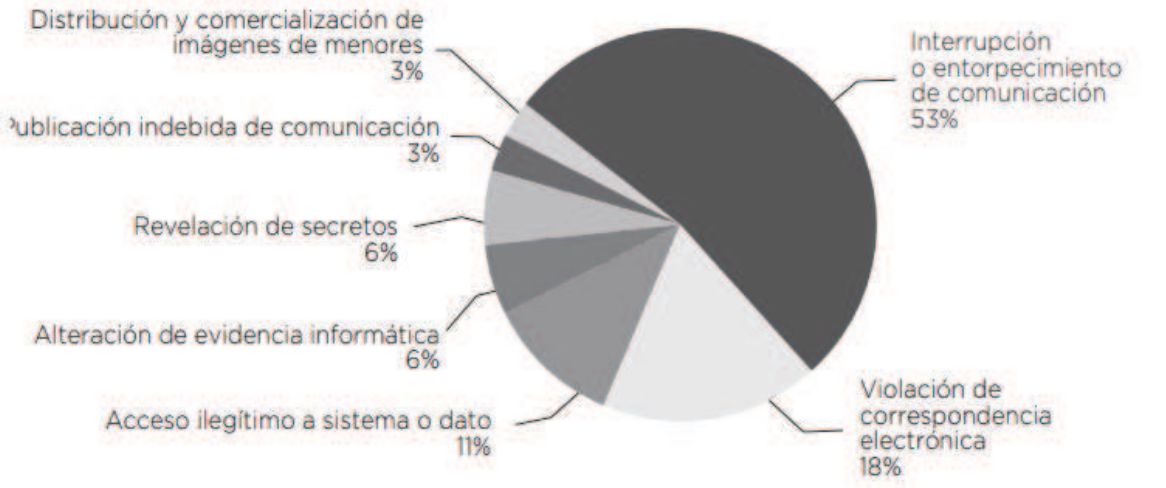
Tabla 3. Denuncias ley 26.388 por figura penal (total país, 2015, justicia federal)

Figura penal	Denuncias
Art. 197 CP: interrupción o entorpecimiento de comunicaciones	60
Art. 153 CP: violación de correspondencia electrónica	20
Art. 153 bis CP: acceso ilegítimo a sistema o dato informático	12
Art. 255 CP: alteración de evidencia informática	7
Art. 157 CP: revelación de secretos	7
Art. 155 CP: publicación indebida de comunicaciones	3
Art. 128 CP: distribución o comercialización de imágenes de menores	3
TOTAL	**112**

Fuente: Ministerio Público Fiscal de la Nación.

En relación a las denuncias por figura penal, al igual que los años anteriores, la mayor cantidad de denuncias federales sobre delitos informáticos se encuadran bajo la figura de interrupción o entorpecimiento de comunicaciones con el 53% del total –60 presentaciones sobre 112–. En 2013, 7 de cada 10 denuncias –71%– estaba relacionada con esta figura, lo que demuestra una disminución en su porcentaje, pero similar al año 2014, donde poco menos de la mitad –46% del total de causas– correspondieron a esta figura.

Gráfico 5. Denuncias ley 26.388 por figura penal (total país, 2015, justicia federal)



La segunda figura sigue siendo la violación de correspondencia electrónica con un 18% del total –20 denuncias durante 2015–. Según los registros del año anterior, 1 de cada 4 causas se relacionan con esta figura.

Una de cada 10 denuncias se engloba bajo el acceso ilegítimo a datos o sistema informático, con la misma cantidad de causas iniciadas en 2014, 12 en total.

Por último, comentaremos los datos publicados en relación al estado de trámite de las causas en el país (justicia federal).

Tabla 4. Denuncias ley 26.388 por estado de trámite (total país, 2015, justicia federal)

Estado de trámite	Denuncias
En trámite	54
Archivo	37
Delegada por incompetencia	8
Sobreseimiento por dif. motivos	5
Desestimada	4
Sobreseimiento por extinción de la acción	3
Acumulación/conexidad	1
TOTAL	**112**

Fuente: Ministerio Público Fiscal de la Nación.

De la presente información, puede afirmarse que casi de la mitad de las causas tramitadas durante 2015 se encontraban en trámite en los tribunales federales de todo el país, donde 54 causas de un total de 112 estaban en esa situación hasta el 31 de diciembre de ese año. Las mismas representan un 48% del total, mientras que en 2014 un 54% se encontraba en esa condición al finalizar ese año.

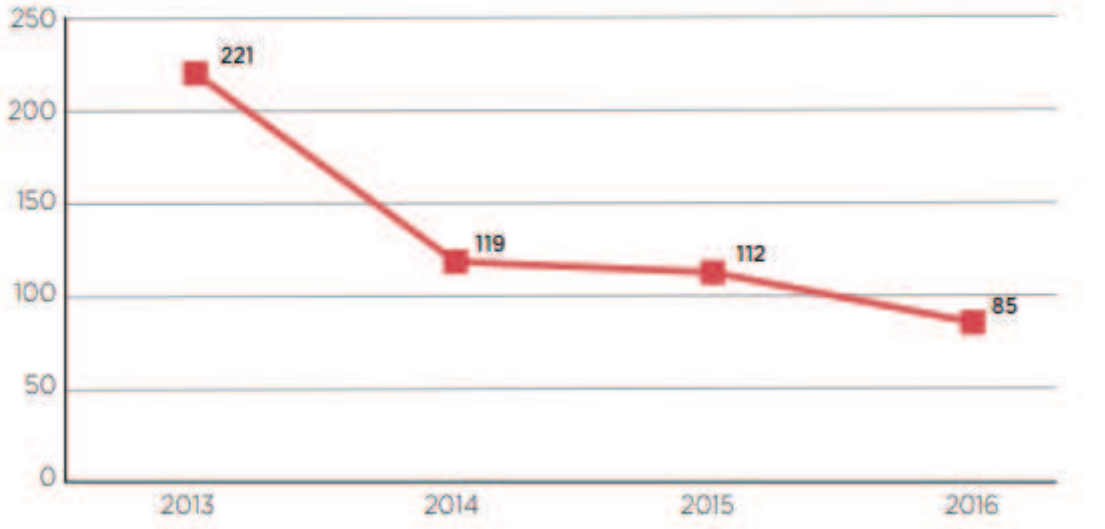
Que, 1 de cada 3 denuncias fue archivada en el período analizado, un tercio de las presentaciones iniciadas –33%– sin discriminar los motivos de tal decisión. El año anterior un 29% de los registros de denuncias fue desestimado. Que, un 7% de las causas –8 en total– fue delegada por incompetencia, lo que demuestra un bajo porcentaje de derivaciones a otros juzgados. Que, un 4% de las causas sentencia el sobreseimiento de las personas imputadas y/o procesadas y otro 4% es desestimado por diferentes motivos especificados estadísticamente. Que, al igual que en 2014, no existen condenas en las causas iniciadas hasta el 31 de diciembre de 2015.

El cuarto muestreo[109] fue publicado oficialmente en Marzo de 2019 bajo el título "Estudios estadísticos sobre cibercrimen: Tercer muestreo de denuncias judiciales de la República Argentina Año 2016", dirigido por Gustavo Sain.

Teniendo la misma dinámica que los muestreos anteriores y buscando destacar sólo los datos que son de interés para nuestra presente tesis, destacaremos los resultados obtenidos en el mismo en el fuero federal, dejando excluidos los datos aportados sobre la situación específica en Ciudad Autónoma de Buenos Aires y en las demás provincias.

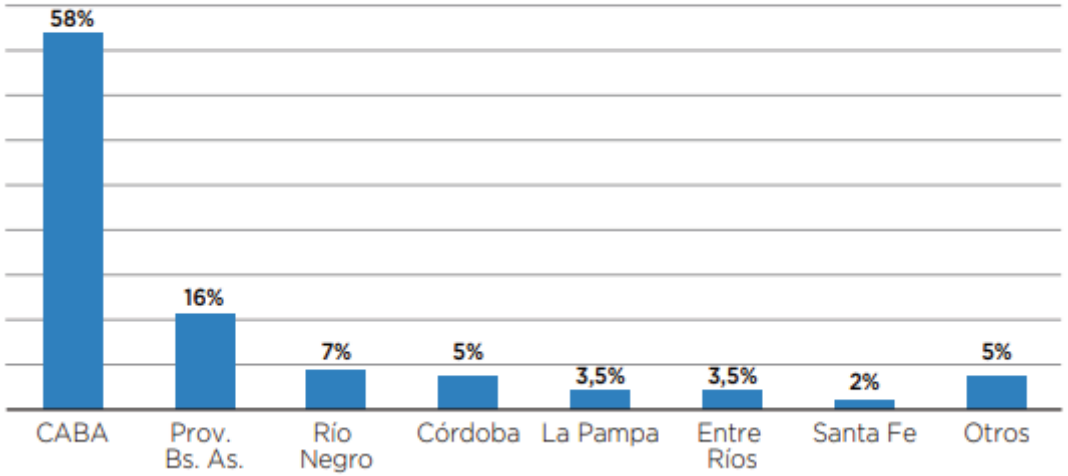
En relación al alcance de este tercer muestreo, y al igual que en los anteriores, se realizó un relevamiento estadístico de denuncias registradas en los fueros criminales y correccionales de la provincia de Buenos Aires en base a la estadística brindada por la Procuración General de la Suprema Corte de Justicia, las presentaciones recibidas por la fiscalía especializada en delitos informáticos de la Ciudad Autónoma de Buenos Aires y las causas iniciadas por los tribunales federales en todo el país de acuerdo a datos aportados por el Ministerio Público Fiscal de la Nación.

Gráfico 2. Denuncias ley 26.388 (total país, 2013 a 2016, justicia federal)



[109] Dirección Nacional de Política Criminal en materia de Justicia y Legislación Penal, Secretaría de Justicia, Ministerio de Justicia y Derechos Humanos de la Nación Argentina, "Tercer muestreo de denuncias judiciales de la República Argentina : Año 2016" / Gustavo Sain. - 1a ed . - Archivo Digital: descarga y online ISBN 978-987-4196-80-4; Ciudad Autónoma de Buenos Aires : Ediciones SAIJ, Publicado en Marzo 2019

Gráfico 3. Denuncias ley 26.388 por distrito (total país, 2016, justicia federal)



Al igual que los últimos cuatro años, la mayor cantidad de ingresos de causas vinculadas a figuras de la ley 26.388 se iniciaron en la Ciudad Autónoma de Buenos Aires, con un total de 49 denuncias sobre 85 –14 menos que el 2015–. En términos de porcentajes, representa el 58% del total, casi el mismo porcentaje que el año anterior –56%–. Nuevamente, más de la mitad de las denuncias federales se registran en la capital del país.

El segundo distrito con mayor cantidad de denuncias sigue siendo la provincia de Buenos Aires, con 14 presentaciones, un 16% del total –el año 2015 fue de 15%–. Si se suman las causas con las de la Ciudad Autónoma de Buenos Aires, 3 de cada 4 denuncias se concentran en estas dos jurisdicciones, con un 74%.

El 16% restante de denuncias se distribuyen en forma equitativa en 14 provincias, siendo la provincia de Río Negro, por primera vez, la tercera jurisdicción con 6 causas –7% del total– y seguida por Córdoba con cuatro denuncias –5%–. El resto poseen entre tres y un ingreso anual por este tipo de delitos.

Tabla 3. Denuncias ley 26.388 por figura penal (total país, 2016, justicia federal)

Figura penal	Denuncias
Art. 197 CP: interrupción o entorpecimiento de comunicaciones	38
Art. 153 CP: violación de correspondencia electrónica	22
Art. 153 bis CP: acceso ilegítimo a sistema o dato informático	9
Art. 255 CP: alteración de evidencia informática	8
Art. 157 CP: revelación de secretos	6
Art. 155 CP: publicación indebida de comunicaciones	2
TOTAL	**85**

Fuente: Ministerio Público Fiscal de la Nación

Gráfico 5. Denuncias ley 26.388 por figura penal (total país, 2016, justicia federal)



Al igual que los datos de los informes previos, la mayor cantidad de denuncias federales sobre delitos informáticos se encuadran bajo la figura de interrupción o entorpecimiento de comunicaciones con el 45% del total –38 presentaciones sobre 85–. Esto registra una caída de un 8% a comparación del año anterior. Cabe señalar que en 2013, 7 de cada 10 denuncias –71%– estaba relacionada con esta figura, lo que demuestra una disminución en su porcentaje.

La segunda figura sigue siendo la violación de correspondencia electrónica con un 26% del total –22 denuncias durante 2016–. Esto representa 1 de cada 4 presentaciones.

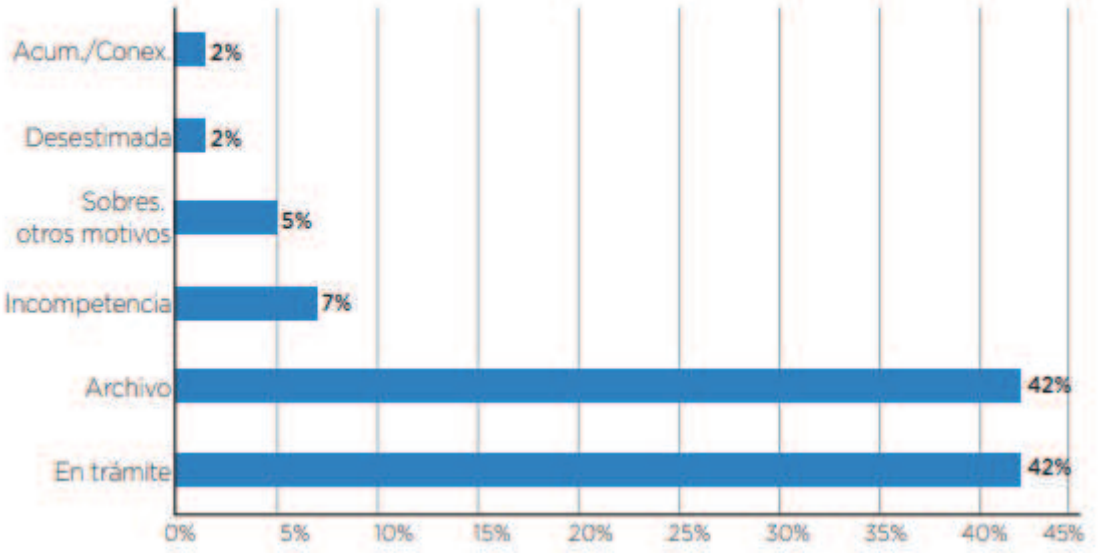
Una de cada 10 denuncias se engloba bajo el acceso ilegítimo a datos o sistema informático, con 8 causas iniciadas en 2016.

Tabla 4. Denuncias ley 26.388 por estado de trámite (total país, 2016, justicia federal)

Estado de trámite	Denuncias
En trámite	36
Archivo	36
Delegada por incompetencia	6
Sobreseimiento por diferentes motivos	5
Desestimada	1
Acumulación/conexidad	1
TOTAL	**85**

Fuente: Ministerio Público Fiscal de la Nación.

Gráfico 6. Denuncias ley 26.388 por estado de trámite (total país, 2016, justicia federal)



A diferencia que en el período anterior, donde casi de la mitad de las causas tramitadas durante 2015 se encontraban en trámite en los tribunales federales de todo el país, durante 2016 un porcentaje menor de la causas se encuentran en esa condición –42%–. En 2015, 54 causas de 112 estaban en esa situación, lo que

representaba un 48% del total, mientras que en 2014 un 54% se encontraban en esa condición.

Que, 4 denuncias de cada 10 fueron archivadas en el período analizado –42%–, un porcentaje mayor que en 2015 donde un tercio de las presentaciones iniciadas –33%– fueron sometidas a esa decisión.

Que, al igual que el período anterior, un 7% de las causas –6 en total– fue delegada por incompetencia. Por último, un 5% de las causas sentencian el sobreseimiento de las personas imputadas y/o procesadas y otro 4% son desestimadas por diferentes motivos no especificados estadísticamente.

Que, al igual que en 2014 y 2015, no existen condenas en las causas iniciadas hasta el 31 de diciembre de 2016.

El quinto muestreo[110] ha sido publicado oficialmente en Julio de 2019 bajo el título "Estudios estadísticos sobre cibercrimen: Tercer muestreo de denuncias judiciales de la República Argentina Año 2017", dirigido por Gustavo Sain.

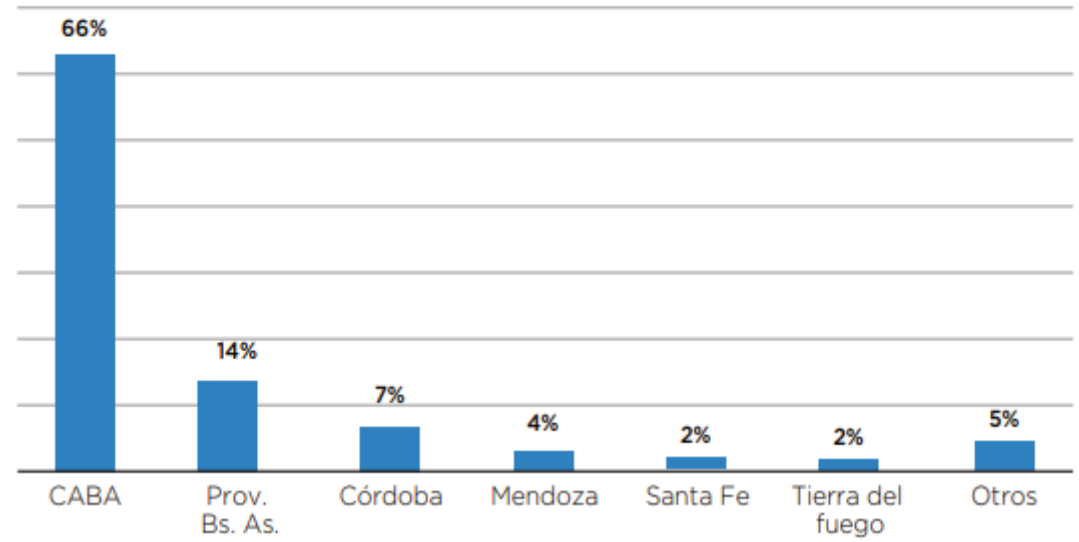
Teniendo la misma dinámica que los muestreos anteriores y buscando destacar sólo los datos que son de interés para nuestra presente tesis, destacaremos los resultados obtenidos en el mismo en el fuero federal, dejando excluidos los datos aportados sobre la situación específica en Ciudad Autónoma de Buenos Aires y en las demás provincias.

En relación al alcance de este tercer muestreo, y al igual que en los anteriores, se realizó un relevamiento estadístico de denuncias registradas en los fueros criminales y correccionales de la provincia de Buenos Aires en base a la estadística brindada por la Procuración General de la Suprema Corte de Justicia, las presentaciones recibidas por la fiscalía especializada en delitos informáticos de la Ciudad Autónoma de Buenos Aires y las causas iniciadas por los tribunales federales en todo el país de acuerdo a datos aportados por el Ministerio Público Fiscal de la Nación.

[110] Dirección Nacional de Política Criminal en materia de Justicia y Legislación Penal, Secretaría de Justicia, Ministerio de Justicia y Derechos Humanos de la Nación Argentina, "Tercer muestreo de denuncias judiciales de la República Argentina : Año 2016" / Gustavo Sain. - 1a ed . - Archivo Digital: descarga y online ISBN 978-987-4196-80-4; Ciudad Autónoma de Buenos Aires : Ediciones SAIJ, Publicado en Marzo 2019

En los muestreos anteriores, la estadística reportada por el Ministerio Público Fiscal de la Nación se remitió a cantidad de causas iniciadas relacionadas con las figuras de la ley 26.388 en los tribunales federales de todo el país. Durante el año 2017, los datos informados refieren, en cambio, a la cantidad de delitos investigados bajo las figuras de la norma en cuestión, lo que impide la comparación con las cifras de los años anteriores.En este sentido, durante el año 2017 se investigaron 205 delitos relacionados con las figuras penales contempladas en la "Ley de delitos informáticos"

Gráfico 1. Denuncias ley 26.388 por distrito (total país, 2017, justicia federal)



Al igual que desde el año 2013, la mayor cantidad de ingresos de causas vinculadas a figuras de la ley 26.388 se iniciaron en la Ciudad Autónoma de Buenos Aires, con un total de 136 delitos investigados sobre 205. En este sentido, 3 de cada 4 denuncias investigadas en la justicia federal se concentran en este distrito, lo que marca una clara centralización urbana en la capital del país para este tipo de delitos.

El segundo distrito con mayor cantidad de denuncias vuelve a ser la provincia de Buenos Aires, con 29 presentaciones, un 14% del total. Si se suman las causas con las de la Ciudad Autónoma de Buenos Aires, el 80% de las investigaciones se concentran en estas dos jurisdicciones.

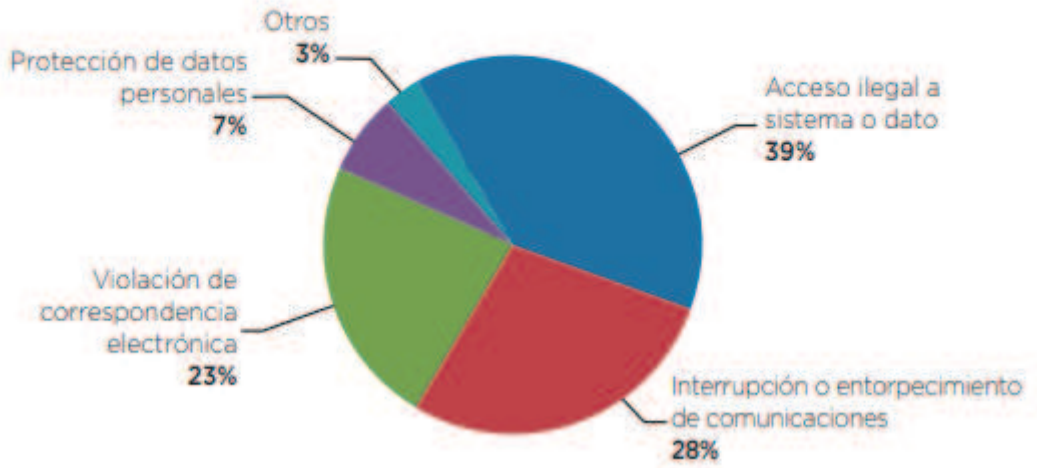
El tercer distrito en importancia de investigaciones de delitos relacionados con las figuras de la ley 26.388 es Córdoba, con un 7% del total, con 15 investigaciones cursadas, seguida por Mendoza con 8 –4%–

Tabla 4. Denuncias ley 26.388 por figura penal (total país, 2017, justicia federal)

Figura penal	Denuncias
Art. 153 bis CP: acceso ilegítimo a sistema o dato informático	80
Art. 197 CP: interrupción o entorpecimiento de comunicaciones	58
Art. 153 CP: violación de correspondencia electrónica	47
Art. 157 bis CP: delitos vinculados con la protección de datos personales	14
Art. 155 CP: publicación indebida de comunicaciones	2
Art. 183 CP: daño a bienes intangibles y distribución de virus	2
Art. 255 CP: alteración de evidencia informática	2
TOTAL	**205**

Fuente: Ministerio Público Fiscal de la Nación.

Gráfico 3. Denuncias ley 26.388 por figura penal (total país, 2017, justicia federal)



A diferencia del período 2013-2016 y con el eje “delitos investigados” y no causas en curso, por primera vez la mayor cantidad de denuncias en curso bajo las figuras de la ley 26.388 es la de acceso ilegítimo a sistema o dato informático, con

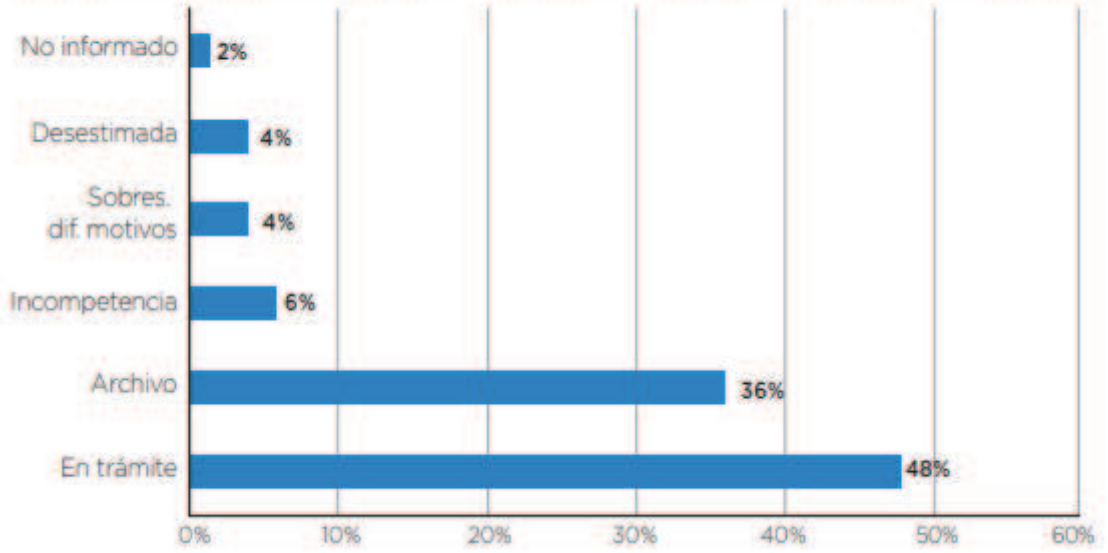
80 hechos investigados por sobre un total de 205, lo que representa casi 1 de cada 4 pesquisas realizadas –39%–.

La segunda figura es aquella que en términos de causas iniciadas ocupó el primer lugar durante los relevamientos anteriores, la interrupción o entorpecimiento de comunicaciones, con 58 hechos investigados, lo que representa el 28% del total de ingresos. Casi un tercio de los ilícitos corresponde a esta modalidad.

La tercera figura en importancia fue la de violación de correspondencia electrónica con un 23% del total –22 denuncias durante 2016–. Casi un cuarto de las presentaciones.

La categoría siguiente en orden de importancia son los delitos vinculados con la protección de datos personales, una figura atípica en cantidad de causas de acuerdo a los registros de los relevamientos anteriores. Bajo los parámetros de delitos investigados, de 205 hechos 14 respondieron a este tipo de hechos.

Gráfico 4. Denuncias ley 26.388 por estado de trámite (total país, 2017, justicia federal)



Casi al igual que el período anterior, el 42% de las causas tramitadas durante 2016 se encontraban en trámite en los tribunales federales de todo el país, durante 2017 casi la mitad de los delitos investigados de la causas se encuentran en esa condición -48%-, con 99 hechos pesquisados por sobre 205.

Durante el año anterior 4 denuncias de acá 10 fueron archivadas -42%- mientras que en 2017 poco más de un tercio -36%- fueron sometidas a esa decisión por diferentes motivos.

Casi en los mismos parámetros que en 2016 (7% de las causas) en el período analizado un 6% –14 hechos investigados– fue delegado por incompetencia.

Por último, un 5% de las causas sentencian el sobreseimiento de las personas imputadas y/o procesadas y otro 4% son desestimadas por diferentes motivos no especificados estadísticamente.

Al igual que en 2014 y 2015, no existen condenas en las causas iniciadas hasta el 31 de diciembre de 2017.

3.4. Los Centros de Respuesta (CSIRT/CERT)

Otro instrumento estatal de recolección de datos en materia de ciberseguridad que podemos mencionar son los CSIRT/CERT[111] (*Computer Emergency Response Team*), concepto que fue inicialmente creado en 1988 por la Universidad de Carnegie Mellon como respuesta al gusano de Internet Morris[112]. Existen diferentes CERT públicos y privados en muchos países y, según FIRST[113] (*Forum of Incident Response and Security Teams*), la entidad que actualmente agrupa y coordina los CERT Internacionales, en Argentina existe un sólo CSIRT/CERT afiliado[114]: CSIRT-BANELCO para entidades bancarias privadas.

[111] Un CSIRT es un centro de respuesta a incidentes de seguridad en tecnologías de la información. Se trata de un grupo de expertos responsable del desarrollo de medidas preventivas y reactivas ante incidencias de seguridad en los sistemas de información. Un CERT estudia el estado de seguridad global de redes y ordenadores y proporciona servicios de respuesta ante incidentes a víctimas de ataques en la red, pública alertas relativas a amenazas y vulnerabilidades y ofrece información que ayude a mejorar la seguridad de estos sistemas.

[112] En Noviembre de 1988 Morris fue el primer ejemplar de malware auto replicable que afectó a Internet.

[113] CERT miembros de FIRST en Argentina, http://www.first.org/members/map/, Consultado: 27 de Noviembre de 2013

[114] A fecha 02/05/2013, según información brindada en FIRST. Url: http://www.first.org/members/teams, Consultado: 27 de Noviembre de 2019

En Argentina, dependiente de la Jefatura de Gabinetes de Ministros, sobre el año 2013 se ha creado el ICIC[115] (ex ArCERT), como el "Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad", mediante la Resolución JGM Nº 580/2011.

Dicho organismo fue generado con finalidad de "*impulsar la creación y adopción de un marco regulatorio específico que propicie la identificación y protección de las infraestructuras estratégicas y críticas del Sector Público Nacional, los organismos interjurisdiccionales y las organizaciones civiles y del sector privado que así lo requieran […]*".

A fin de que los distintos estamentos gubernamentales puedan participar de dicho programa, el mismo establece la posibilidad de adhesión a través de unos formularios puestos a disposición en la Resolución de la Jefatura de Gabinete de Ministros Nº 3/2011. Es decir, dicho centro de respuestas (CERT), ha sido diseñado para recepcionar solamente aquellos reportes de incidentes de seguridad que ocurran en las redes del Sector Público Nacional.

Entre los distintos objetivos determinados para ser llevados a cabo por el ICIC (de acuerdo al Art. 3 de la Resolución JGM Nº 580/2011), vale la pena destacar el inciso *k* y *n*, los cuales se detallan a continuación a efectos didácticos del lector:

k) Centralizar los reportes sobre incidentes de seguridad ocurridos en redes teleinformáticas del Sector Público Nacional que hubieren adherido al Programa y facilitar el intercambio de información para afrontarlos.

n) Elaborar un informe anual de la situación en materia de ciberseguridad, a efectos de su publicación abierta y transparente.

Como puede advertirse en el inc. *k*, el ICIC ha sido constituido con el objetivo de gestionar los incidentes de seguridad ocurridos en los entes del Sector Público Nacional que hubieren adherido. Actualmente también se permite la adhesión de organizaciones civiles y del sector privado (art. 5), aunque no están claros los beneficios de dicha adhesión.

[115] ICIC, *"Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad"*, Url: http://www.icic.gob.ar, Consultado: 27 de Noviembre de 2019

En relación al inc. *n*, puede advertirse la obligación por parte del ICIC de la publicación de un informe anual que, de forma "*abierta y transparente*" (texto propio de la norma), permita a todos los ciudadanos conocer el estado de situación en materia de seguridad informática de los entes del Sector Público Nacional. A más de dos años desde la creación del ICIC (Julio 2011), no se ha podido encontrar ningún informe publicado en virtud de la obligación impuesta por el citado inciso.

Más allá de estos incisos, y a modo general en relación a las funciones del ICIC, se destaca que el mismo no está destinado a recibir denuncias, algo que se han encargado de dejarlo claro y en letras mayúsculas en la publicación de la "Guía Práctica para realizar denuncias ante un posible delito informático"[116], en donde textualmente dice: "*RECUERDE – El ICIC no recibe denuncias. Asesora y recomienda*"

En el asesoramiento realizado para el ciudadano víctima de delitos informáticos en la citada guía, se pueden leer los siguientes pasos a seguir:

1. No borre, destruya, o modifique la información que posea en su computadora relacionada al hecho. Recuerde que siempre, la integridad de la información es vital para poder seguir adelante con las causas penales que se inicien.

2. Nunca reenvíe los mensajes (correos electrónicos) constitutivos del delito.

3. Realice inmediatamente la denuncia ante la dependencia policial más cercana a su domicilio (Comisaría de su barrio en cualquier lugar del país). Recuerden que tienen la obligación de tomar su denuncia.

A los fines de resguardar correctamente la prueba, una vez realizada la denuncia, proceda de la forma en que el investigador le indique.

El punto medular del asesoramiento se encuentra en el punto 3: *realizar la denuncia en la dependencia policial más cercana al domicilio de la víctima.* Este aspecto, que puede ser considerado como simple, en una gran parte de nuestro país representa un problema en sí mismo, atento al desconocimiento y falta de capacitación que existe por parte de los agentes policiales.

[116] ICIC, "Guía Práctica para realizar denuncias ante un posible delito informático". Url: http://www.icic.gob.ar/archivos/instructivo_denuncias.pdf, Consultado: 27 de Noviembre de 2019

En la Provincia de Santa Fe, por citar un caso difundido mediáticamente, un importante médico de la zona fue víctima de un caso de hacking[117]. El Dr. Arturo Serrano (víctima) afirmó en varias entrevistas haber intentado denunciar ante diferentes comisarías, sin lograr que en alguna de ellas le tomaran la denuncia por el hecho ocurrido.

En países con mayor desarrollo, hace años que existen diversos centros de respuesta para los casos de delincuencia informática. Por citar algunos, se pueden mencionar el IC3[118] de Estados Unidos, la UNEDEI[119] en México, la CYCO[120] en Suiza. Todos ellos, además de contar con una infraestructura dedicada a la recepción de denuncias por parte de las víctimas, permiten que las propias denuncias puedan ser realizadas de forma electrónica (lo que permite el acceso al "sistema" de muchas más víctimas) e incluso, en algunas de ellas, se permiten las denuncias de tipo anónimo con el fin de fomentar a aquellos que han sido víctimas pero no quieren formar parte del proceso, o bien, desean reportar el incidente resguardando la confidencialidad de sus datos (un aspecto que posteriormente será tratado).

A nivel de normativa internacional, se debe destacar que en la Convención de Cibercriminalidad de Budapest[121] -instrumento jurídico internacional de mayor importancia que ya hemos mencionado- en su art. 35 obliga a a los Estados firmantes -entre los cuáles Argentina ya forma parte por Ley Nro. 24.711- a la adopción de un Centro de Respuestas 24x7, a fines de determinar un punto de

---

[117] DIARIO UNO Santa Fe, "Hackearon el mail de un santafesino para estafar a sus contactos". 05/08/2013. Url: http://www.unosantafe.com.ar/santafe/Hackearon-el-mail-de-un-santafesino-para-estafar-a-sus-contactos-20130805-0018.html, Consultado: 27 de Noviembre de 2013

[118] INTERNET CRIME COMPLAINT CENTER (IC3), en Estados Unidos fue establecido por una asociación entre el FBI y el NW3C (National White Collar Crime Center). Url: http://www.ic3.gov, Consultado: 27 de Noviembre de 2013

[119] UNIDAD ESTATAL DE DELITOS ELECTRÓNICOS E INFORMÁTICOS, Fiscalía General de Chihuahua, México. Url: http://fiscalia.chihuahua.gob.mx/intro/?page_id=3029, Consultado: 27 de Noviembre de 2013

[120] CYBERCRIME COORDINATION UNIT SWITZERLAND (CYCO), Suiza. Url: http://www.cybercrime.admin.ch/content/kobik/en/home/meldeformular.html, Consultado: 27 de Noviembre de 2013

[121] COUNCIL OF EUROPE. "Convenio de Cibercriminalidad de Budapest". Budapest, 23 de noviembre de 2001. Url: http://www.coe.int/t/dghl/standardsetting/t-cy/ETS_185_spanish.pdf , Consultado: : 10 de Abril de 2017

contacto de trabajo que permita la colaboración internacional en casos de cibercrimen.

3.5. Estadísticas a nivel internacional.

En el ámbito internacional, nuevamente recurriremos a uno de los estudios más importantes que hemos encontrado, citado anteriormente en el análisis normativo. Nos referimos al trabajo *Comprehensive Study on Cybercrime*[122] -o estudio exhaustivo sobre cibercrimen- realizado por Naciones Unidas, en particular por la United Nations Office on Drugs and Crime (ONUDC), en el cuál recordamos que se encuestaron más de 82 países, incluyendo varios de Latinoamérica (entre ellos, Argentina).

De acuerdo a este estudio de Naciones Unidas, a nivel mundial los actos delictivos cibernéticos muestran una distribución amplia entre actos con motivaciones financieras, actos relacionados con contenidos informáticos y actos contra la confidencialidad, integridad y accesibilidad de los sistemas informáticos.

Sin embargo, y de acuerdo al precitado estudio, los gobiernos y las empresas del sector privado perciben la amenaza y el riesgo relativos de manera diferente. Actualmente las estadísticas delictivas registradas por la policía no representan una base sólida para hacer comparaciones entre países, aunque dichas estadísticas a menudo son importantes para hacer políticas a nivel nacional. Dos terceras partes de los países consideran sus sistemas de estadística policial como insuficientes para registrar el delito cibernético. Las tasas de delito cibernético registradas por la policía están asociadas con los niveles de desarrollo del país y la capacidad especializada de la policía, y no con las tasas delictivas subyacentes.

Por estos motivos, el estudio afirma que las encuestas de victimización representan una base más sólida para la comparación. Estas muestran que la victimización individual por delito cibernético es mucho mayor que por las formas de

[122] NACIONES UNIDAS, New York, 2013. UNODC. Comprehensive Study on Cybercrimen. Url: http://www.unodc.org/documents/organizedcrime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf. Consultado: 27 de Noviembre de 2019

delitos 'convencionales'. Las tasas de victimización por fraude en línea con tarjetas de crédito, robo de identidad, respuesta a intentos de suplantación (phishing) y por experimentar acceso no autorizado a una cuenta de correo varían entre el 1% y el 17% de la población con acceso a Internet de 21 países de todo el mundo, en comparación con tasas de robo, asalto y robo de coches de menos de 5 por ciento en los mismos países.

A nivel general las tasas de victimización por delitos cibernéticos son más altas en los países con niveles menores de desarrollo, lo que destaca la necesidad de fortalecer los esfuerzos de prevención en esos países.

Las empresas del sector privado en Europa reportan tasas de victimización similares – entre el 2% y el 16% –por actos como el acceso no autorizado a los datos por intrusión o phishing. Las herramientas delictivas para estos delitos, como las redes zombi o "botnets", tienen un alcance mundial. En 2011 más de un millón de direcciones IP únicas a nivel mundial funcionaban como servidores de mando y control de redes *zombie* o "botnet".

El contenido en Internet también representó una inquietud considerable para los gobiernos. El material al que se dirigen los esfuerzos de remoción no solo incluye la pornografía infantil (abuso sexual infantil) y el discurso de incitación al odio, sino también contenido relacionado con la difamación y la crítica a los gobiernos, lo cual despierta en algunos casos inquietudes relacionadas con las leyes de derechos humanos. Se calcula que casi el 24% de todo el tráfico mundial de Internet viola los derechos de autor, con las descargas de material compartido de pares a pares (P2P) particularmente numerosas en países de África, América del Sur y Asia Occidental y Austral.

3.5.1. El problema de la victimización y la falta de denuncias

Continuando con el análisis del precitado estudio exhaustivo de Naciones Unidas, el mismo afirma que más del 90 por ciento de los países encuestados reportan que los actos de delito cibernético llegan con mayor frecuencia a la

atención de las autoridades a través de denuncias de víctimas, ya sea a título individual o empresas.

Los Estados encuestados calculan que la proporción de victimización real por delito cibernético reportada a la policía era superior al 1 por ciento. Una encuesta mundial del sector privado sugiere que el 80 por ciento de las víctimas de los principales delitos cibernéticos no denuncian el delito a la policía. Este último dato sobre el nivel de la cifra negra en delitos informáticos confirma una de nuestras hipótesis de trabajo, que luego buscaremos validar con mayor nivel de rigurosidad académica.

Se argumenta que el déficit de denuncias se debe (entre otras causas, agregamos nosotros) a una falta de conciencia sobre la victimización y de conocimiento de los mecanismos de denuncia, a la vergüenza y bochorno de la víctima y a los posibles riesgos para la reputación de las compañías.

Las autoridades de todas las regiones del mundo destacaron las iniciativas para favorecer las denuncias, incluyendo sistemas de denuncia en línea y telefónica, campañas de concientización pública, los vínculos con el sector privado y una mejor comunicación e intercambio de información por parte de la policía.

Sin embargo, la respuesta al delito cibernético en caso de incidentes debe ir acompañada de investigaciones estratégicas y tácticas a mediano y largo plazo que se enfoquen en los mercados delictivos y en los arquitectos de los esquemas delictivos. En los países desarrollados, las autoridades encargadas de hacer cumplir la ley realizan estas tareas, incluso mediante unidades encubiertas cuyos objetivos son los transgresores en las páginas de redes sociales, salas de chat y los servicios de mensajería instantánea y los servicios P2P. Los desafíos en la investigación del delito cibernético surgen a partir de las innovaciones delictivas de los transgresores, de las dificultades de acceso a la evidencia electrónica, y de las limitaciones en materia de recursos internos, capacidad y logística.

3.6. La medición del delito

Podríamos comenzar preguntándonos sobre ¿Por qué medir el delito cibernético? Entre las respuestas, podríamos citar el Artículo 11 de las Directrices de las Naciones Unidas para la Prevención del Delito[123] donde se declara que "*las estrategias, políticas, programas y medidas de prevención del delito deben tener una amplia base de conocimientos multidisciplinarios sobre los problemas de la delincuencia*".

Esta base de conocimientos debe incluir el establecimiento de "sistemas de datos", es decir, la recopilación de datos para la planeación de intervenciones para prevenir y reducir el delito es tan importante para el delito cibernético como lo es para otros tipos de delito.

La utilidad de la medición del delito cibernético radica en que puede ser usada en las iniciativas de reducción del delito; para fortalecer las respuestas locales, nacionales, regionales e internacionales; para identificar brechas en las respuestas; para ofrecer inteligencia y evaluaciones de riesgos; y para educar e informar al público[124].

Algunos autores han trabajado ya los desafíos particulares de recopilar información sobre la naturaleza y el alcance del delito informático[125]. Según Brenner, debemos atravesar una serie de obstáculos preliminares antes de su medición. Entre ellos encontraremos:

1. Determinar qué constituye "delito informático" (algo de lo que nos hemos ocupado en la primer parte de esta tesis);
2. Los desafíos que representa la falta de denuncias y de registros;

[123] Directrices para la prevención del delito, anexo a la Resolución 2002/13 del Consejo Económico y Social de Naciones Unidas en Medidas para promover la prevención eficaz del delito, 24 de julio de 2002.

[124] FAFINSKI, S., Dutton, W.H. and Margetts, H., 2010. Mapping and Measuring Cybercrime. Oxford Internet Institute Forum Discussion Paper No. 18., Junio de 2010.

[125] Brenner, S.W., 2004. Cybercrime Metrics: Old Wine, New Bottles? Virginia Journal of Law & Technology, 9(13):1-52. El delito cibernético también está incluido como ejemplo de un tipo de 'delito emergente y difícil de medir' en documentos de la 42a Sesión de la Comisión Estadística de las Naciones Unidas. Ver Consejo Económico y Social de las Naciones Unidas, Comisión Estadística, 2012. Informe del Instituto Nacional de Estadística y Geografía de México sobre Estadísticas Delictivas. E/CN.3/2012/3, 6 de diciembre de 2011.

3. Problemas metodológicos de las encuestas y de concientización;
4. Posibles conflictos de intereses en los datos del sector privado.

De acuerdo a este autor, existen cuatro fuentes de información principales para la medición de "qué" actos de delito cibernético ocurren y "qué tanto" ocurren:

(i) las estadísticas delictivas registradas por la policía;

(ii) encuestas basadas en la población y empresariales;

(iii) iniciativas de denuncia para las víctimas; y

(iv) información sobre seguridad cibernética con base tecnológica.

La lista no es exhaustiva, pero cubre las principales fuentes de información que en cierto grado pueden ser comparables de un país a otro. Otras fuentes incluyen los estudios individuales sobre ciertos fenómenos seleccionados, como las técnicas de barrido de los URL, o los asaltos de redes zombie o "botnet".

A continuación, realizaremos un repaso por los cuatro tipos de fuentes analizados en el Anexo II[126] titulado "Medición del delito cibernético", cuya importancia para este trabajo resulta fundamental.

3.6.1. Estadísticas delictivas registradas por la policía

Las estadísticas delictivas registradas por la policía normalmente son consideradas las estadísticas administrativas más cercanas a los eventos delictivos reales[127]. No obstante, como es bien sabido, estas estadísticas sólo capturan los eventos que llegan a ser conocidos por la policía. Como resultado, normalmente ocultan una (a menudo considerable) "cifra negra" del delito[128].

En los eventos de delito cibernético, la diferencia entre victimización y los delitos registrados por la policía puede ser de varios órdenes de magnitud. La

[126] NACIONES UNIDAS, New York, 2013. UNODC. Comprehensive Study on Cybercrimen. Url: http://www.unodc.org/documents/organizedcrime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf, Consultado: 27 de Noviembre de 2019

[127] NACIONES UNIDAS, 2003. Manual para la elaboración de un sistema de estadísticas sobre justicia penal.

[128] NACIONES UNIDAS, Décimo segundo Congreso sobre Prevención del Delito y Justicia Penal. 2010. Situación de la delincuencia y la justicia penal en el mundo. Informe del Secretario General. A/CONF.213/3. 1 Febrero de 2010.

victimización por fraude en línea con tarjetas de crédito de consumidores reportada en encuestas a la población, por ejemplo, podría ser más de 80 veces mayor al número total de fraudes y falsificaciones informáticas registrado por la policía en el mismo país[129].

De acuerdo con una encuesta a la población de casi 20.000 usuarios individuales de Internet en 24 países, solo el 21% de los que respondieron que habían sido víctimas de cualquier acto de delito cibernético indicaron que lo denunciaron a la policía[130].

Una dificultad adicional con las estadísticas delictivas registradas por la policía es el desarrollo de un enfoque comparable de un país a otro para identificar la inclusión de sistemas o datos informáticos en un acto en particular. Los sistemas de denuncia de la policía nacional, basados en incidentes, tienen varias maneras de registrar un acto como el ciberdelito.

Los campos para registrarlo pueden usar indicadores como “si la computadora era el objeto del delito” o “si el delincuente usó equipo informático para perpetrar el delito”[131].

Otros enfoques se basan simplemente en artículos de la legislación penal nacional, y por lo tanto solo cubren un número limitado de actos de delito cibernético, como el “uso indebido de las computadoras”[132].

Esto genera estadísticas policíacas que van desde la proporción de actos comunes en los que una computadora haya sido la herramienta o el objeto, hasta estadísticas sólo de delitos específicamente tecnológicos[133]. En el primero de estos

---

[129] NACIONES UNIDAS, Cálculos de UNODC basados en el cuestionario de delito cibernético del Estudio. P30; y Symantec. 2012. Informe sobre cibercrimen de Norton 2012.
[130] SYMANTEC, 2011. Informe sobre cibercrimen de Norton 2011.

[131] DEPARTAMENTO DE JUSTICIA DE LOS ESTADOS UNIDOS; Buró Federal de Investigaciones. 2000. National Incident-Based Reporting System. Volume 1: Data Collection Guidelines. Disponible en: http://www.fbi.gov/about-us/cjis/ucr/ucr

[132] Ver, por ejemplo, Comisión Económica de las Naciones Unidas para Europa, Conferencia de Estadísticos Europeos. Principios y marco para la clasificación internacional de los delitos con fines estadísticos. ECE/CES/BUR/2011/NOV/8/Add.1. 11 de octubre de 2011. El Anexo I resume los sistemas nacionales de clasificación de delitos.

[133] CANADIAN CENTRE FOR JUSTICE STATISTICS. 2002. Cybercrime: Issues, Data Sources and Feasibility of Collecting Police-Reported Statistics.

casos, puede ser un desafío entender el umbral, y el significado, del uso del equipo informático para perpetrar un delito particular. En el último de los casos, solo se pueden hacer comparaciones de un país a otro cuando la legislación nacional –y las categorías correspondientes usadas para fines estadísticos– sean equivalentes. Para comprender, por ejemplo, si las estadísticas policiacas del "uso no autorizado de una computadora" en un país pueden ser comparadas con las estadísticas de "acceso ilegal a una computadora" de otro país, es necesario examinar los elementos subyacentes del delito en las leyes penales correspondientes. Las comparaciones metodológicamente defendibles de las estadísticas policíacas del "delito cibernético", por lo tanto, son un desafío considerable.

De los países que respondieron a las preguntas sobre las estadísticas policíacas en el informe de la ONU previamente citado, en los 14 actos de delito cibernético (y 3 categorías), menos del 40% indicó que hubiera estadísticas de delitos registrados. Menos del 20% de los campos posibles de datos –en todos los actos de delito cibernético y años– fueron respondidos. Esto podría indicar que muchos países experimentan desafíos considerables en la recopilación de estadísticas policíacas sobre actos de delito cibernético.

Cuando se les preguntaron las razones por las que no había estadísticas, varios países mencionaron desafíos en el desglose o el agrupamiento –ya fuera que los actos solicitados no podían ser separados de los eventos registrados, o que los datos existentes no pudieran ser recopilados fácilmente en las categorías usadas por el cuestionario.

Esto muestra las dificultades en la identificación de una clasificación común de los delitos cibernéticos que pueda usarse para fines estadísticos. Muchos países vincularon los desafíos en las estadísticas policiales con los marcos legales, destacando que la ausencia de una disposición legal específica significa que no hay una categoría correspondiente en las estadísticas policíacas.

En los casos en los que no exista una disposición específica, algunos países ofrecieron cálculos. Un país, por ejemplo, dio el número total de delitos de fraude o falsificación registrado por la policía, junto con un cálculo del porcentaje que fue cometido con el uso de un sistema informático. Por ejemplo, un país dijo que '*las limitaciones de recursos y la naturaleza compleja del 'delito cibernético' hace que*

sea difícil reunir y analizar información estadística de manera que ofrezcan a los gobiernos, el sector privado y los usuarios de tecnología una imagen completa y precisa del problema. Los elementos del 'delito cibernético' a menudo son incidentales a otros delitos penales, muchos casos nunca son notados por las víctimas, o si son notados, no son denunciados (o, si son denunciados, es solo a los proveedores del servicio o las compañías de las tarjetas de crédito y no a las autoridades públicas). Un problema adicional en esta área es el hecho de que muchos de los delitos son de origen transnacional o incierto, y muchos delitos involucran víctimas en masa, lo cual arroja una imagen estadística diferente dependiendo de lo que se cuente: el solo hecho de enviar un correo fraudulento a millones de direcciones podría ser contado como uno o varios millones de intentos, por ejemplo, y podría generar miles de delitos materializados si el esquema delictivo resulta exitoso'.

La revisión de las estadísticas policíacas muestra varios patrones. Primero, hay indicios claros de que –como sugiere la comparación con las encuestas de víctimas a la población– las estadísticas de delito cibernético registradas por la policía no son un buen indicador de los niveles subyacentes de delito cibernético. La tasa de delitos específicamente cibernéticos registrados por la policía podría estar asociada con el nivel de desarrollo de un país y la capacidad de la policía especializada disponible.

El número de países que ofreció datos es comparativamente pequeño. Sin embargo, en ese grupo limitado de países, los que tenían más policía especializada en delito cibernético registra un número más elevado de delitos cibernéticos –al menos de fraude o falsificación informática. La comparación se muestra usando el número de policías especializados y el número de delitos registrados por cada 100.000 usuarios de Internet en cada país, para ofrecer un denominador justo para la comparación.

Este patrón probablemente se explica con el hecho de que son muy pocos los ciberdelitos que llegan a la atención de la policía, y ese porcentaje probablemente podría aumentar con el uso de recursos y capacidad investigativa adicional.

Un segundo patrón está relacionado con las estadísticas de la policía y el desarrollo del país. Cuatro tipos de actos de delito cibernético registrados por la policía –fraude o falsificación informática, delitos de pornografía infantil, acceso ilegal

a un sistema informático e interferencia ilegal de los datos o interferencia con un sistema– son consistentemente más altos por cada 100.000 usuarios de Internet en un grupo de países con muy altos niveles de desarrollo humano, que en un grupo de países con menor nivel de desarrollo humano. La ilustración muestra el número promedio de delitos registrados por la policía por cada 100.000 usuarios de Internet en 15 países con IDH mayor a 0,8, en comparación con 13 países con IDH menor a 0,8. Es posible que los niveles absolutos de al menos algunos de esos delitos sean de hecho más altos en los países más desarrollados.

Los resultados de las encuestas a la población por el fraude informático, por ejemplo, respaldan un nivel de victimización ligeramente más alto en los países más desarrollados. No obstante, las encuestas sugieren una imagen inversa en otros actos de delito cibernético padecidos por individuos – con niveles normalmente más altos de victimización en los países menos desarrollados[134]. La imagen de los recursos de la policía, combinada con el hecho de que el comparador del homicidio registrado por la policía[135] es mayor en el grupo de países menos desarrollados, podría sugerir que una capacidad investigativa mayor de la policía para el delito cibernético en los países desarrollados es responsable, en parte, de influir en las grandes diferencias entre los dos grupos de países examinados.

Para cerrar con esta primera categoría de estadísticas analizada por el estudio de Naciones Unidas, dejamos una apreciación realizada sobre la suficiencia del sistema estadísticas policíacas que cada país tenía para registrar los delitos informáticos.

En su respuesta, dos tercios de los países encuestados consideraron que su sistema nacional no era suficiente. Los encuestados destacaron que los sistemas policíacos de registro de estadísticas podrían ser mejorados de varias maneras[136].

[134] Por ejemplo, con relación a la pornografía, ver UNODC. 2010. La globalización del delito: evaluación de la amenaza que plantea la delincuencia organizada transnacional. Capítulo 10.

[135] Las tasas de homicidio registradas por la policía son presentadas por cada 100,000 habitantes, no por cada 100,000 usuarios de Internet.

[136] Las formas de mejora señaladas fueron: 1) Instalación de una señal en el sistema de registros para identificar un elemento cibernético de los delitos. 2) Establecimiento de un único ente comunicativo centralizado para las estadísticas de los agentes de la ley y la justicia penal. 3) Desarrollo de reglas de conteo estandarizadas -en particular para actos que tienen como blanco múltiples víctimas (como el phishing). 4) Desarrollo más extenso de los sistemas de clasificación del delito para reflejar el delito cibernético.

A pesar de dichas limitaciones, los países indicaron que las estadísticas del delito cibernético registradas por la policía son importantes para el desarrollo de políticas para combatir el delito cibernético. Un país, por ejemplo, declaró que "cada cuatro años, las estadísticas policíacas, combinadas con información sobre el impacto, la amenaza y la vulnerabilidad de distintos tipos de delitos, incluido el delito cibernético, son analizadas en una Imagen de la Seguridad de la Policía Nacional. Esta imagen es usada para establecer las prioridades de policía y justicia en el Plan Nacional de Seguridad".

Muchos países destacaron que las estadísticas policíacas no deben ser usadas por sí solas. Más bien se les debe combinar con otras fuentes de datos. Los países destacaron que este era especialmente el caso con el delito cibernético, ya que el largo proceso de generación de las estadísticas registradas por la policía podría no ir al paso de los cambios tecnológicos o de los cambios en las tendencias del delito cibernético. Por eso, la información de las evaluaciones periciales de los cambios tecnológicos actuales y previstos, así como la experiencia con los delitos reales y el desarrollo de jurisprudencia, debe ser integrada con las tendencias estadísticas. Otros países mencionaron que las estadísticas del delito cibernético registradas por la policía eran importantes para nutrir los procesos de reforma legislativa, y para elevar la consciencia del público sobre la naturaleza y el alcance del delito cibernético.

3.6.2. Estadísticas a la población y a las empresas

Las encuestas sobre victimización delictiva son promovidas constantemente como la manera más efectiva de recoger estadísticas delictivas. En principio, estas eliminan la incertidumbre de la 'cifra desconocida' de los delitos que no son denunciados a la policía, al reunir información directamente de la población de víctimas potenciales[137]. Al mismo tiempo, las encuestas de victimización delictiva tienen sus propios desafíos metodológicos, incluida la necesidad de identificar de manera precisa a la población objetivo, de diseñar un instrumento de sondeo y un marco de muestra apropiados, y de abordar de manera adecuada las no respuestas.

[137] NACIONES UNIDAS, Manual para encuestas de victimización., UNODC/UNECE. 2010.

No obstante, cuando se adoptan metodologías y frases estándar para las preguntas, las encuestas de victimización delictiva pueden resultar comparables de un país a otro a un grado razonable.

Las encuestas internacionales y nacionales de victimización por delito no han, hasta la fecha, incorporado sistemáticamente preguntas estandarizadas relacionadas con el delito cibernético.

Algunas encuestas nacionales a la población cubren 'experiencias negativas al usar Internet,[138]' 'incidentes con programas maliciosos'[139] o 'amenazas de daño o ataque informático' o 'fraude en Internet'[140]. Otras encuestas nacionales cubren delitos relacionados que podrían o no involucrar sistemas informáticos o datos incluyendo el 'robo de identidad'[141] y la 'clonación de tarjetas bancarias'[142].

Las organizaciones del sector privado condujeron además encuestas de victimización del delito cibernético padecido por las empresas[143]. Aunque algunas de esas encuestas hacen uso de un marco de muestra estadístico, la mayoría son encuestas a los clientes, o a 'informantes clave' selectos. Varias encuestas nacionales gubernamentales también han cubierto la victimización de las empresas[144]. Además, la encuesta de la Comunidad Eurostat sobre uso de ICT en las empresas recientemente ha cubierto temas de delito cibernético y seguridad

[138] UNITED KINGDOM HOME OFFICE; 2012. Hate crime, cyber security and the experience of crime among children: Findings from the 2010/11 British Crime Survey: Supplementary Volume 3 to Crime in England and Wales 2010/11.

[139] AUSCERT; 2008. Home Users Computer Security Survey 2008.

[140] HONG KONG UNICVS. 2010. Final Report of the 2006 Hong Kong UNICVS.

[141] DEPARTAMENTO DE JUSTICIA DE LOS ESTADOS UNIDOS, Bureau of Justice Statistics. 2008. Identity Theft Supplement to the National Crime Victimization Survey 2008.

[142] INEGI. 2012. Encuesta Nacional de Victimizacíon y Percepcíon sobre Seguridad Pública 2012 (ENVIPE), Cuestionario Principal.

[143] Computer Security Institute. 2011. CSI Computer Crime and Security Survey 2010/2011; PricewaterhouseCoopers. 2012. Global State of Information Security Survey; Ponemon/Check Point Software Technologies. 2012. The Impact of Cybercrime on Business; y Ponemon/HP Enterprise Security. 2012. Cost of Cybercrime Study 2012.

[144] United States Department of Justice, Bureau of Justice Statistics. 2006. National Computer Security Survey; y Australian Institute of Criminology. 2009. The Australian Business Assessment of Computer User Security: A National Survey.

cibernética en un módulo dedicado[145]. Las preguntas realizadas en las encuestas empresariales a menudo usan la frase 'incidente de seguridad' para cubrir un amplio rango de actos de delito cibernético, incluido el acceso ilegal por penetración externa al sistema o pirateo, interferencia a los sistemas/datos bajo la forma de una infección de programa malicioso o un ataque DDoS, fraude informático perpetrado por 'agentes internos', o adquisición ilegal de datos informáticos bajo la forma de una 'violación a la seguridad de los datos'.

Existe una considerable diversidad en el uso de la terminología, en la manera en que se formulan las preguntas y en la inclusión de preguntas relacionadas con el delito cibernético en las encuestas sobre victimización. No es poco raro que se incluyan las preguntas sobre delito cibernético como 'módulos' especiales en las encuestas periódicas sobre victimización –lo cual dificulta armar datos con una cronología. Aunque algunas encuestas sí incluyen a países en desarrollo[146], el enfoque está predominantemente en los países desarrollados, lo cual deja una necesidad urgente de datos de encuestas de una gran parte del mundo. Durante la recopilación de información para el Estudio, pocos países pudieron proveer información sobre encuestas a la población o encuestas empresariales relevantes al delito cibernético. Aunque había datos de encuestas disponibles, parecen haber sido sujetos a distintas críticas –incluyendo las dificultades para obtener una muestra que sea representativa no solo de la población en riesgo, sino también de la población de pérdidas debido al delito cibernético

Será vital un mayor desarrollo de la metodología de las encuestas y de la estructura de sus preguntas para los esfuerzos futuros para medir la naturaleza y el alcance del delito cibernético.

Aunque el delito cibernético es –en algunos aspectos– un delito difícil de medir debido a factores de definición y de falta de concientización, existen precedentes de adaptación de metodologías de encuestas sobre victimización a otros delitos difíciles

[145] Eurostat. 2011. Encuesta de la Comunidad Eurostat sobre uso de ICT y comercio electrónico en las empresas. Disponible en: http://epp.eurostat.ec.europa.eu/statistics_explained/index.php/ICT_security_in_enterprises

[146] Symantec. 2012. Informe sobre cibercrimen de Norton 2012 (incluye Sudáfrica) y PricewaterhouseCoopers. 2011. Cybercrime: Protecting against the Growing Threat. Global Economic Crime Survey (cubre 78 países, incluyendo 13 en África).

de medir, como la violencia contra las mujeres[147]. Además, los avances recientes en la ICVS se han enfocado en probar las metodologías de encuesta en Internet[148] –un paso importante cuando la población de interés son los 'usuarios de Internet'. Una 'hoja de ruta' reciente para mejorar las estadísticas delictivas a nivel nacional e internacional destaca aún más la importancia de desarrollar y probar las encuestas estadísticas para la recolección de datos sobre formas específicas de delito cibernético[149]. Dentro de este Estudio, se usan los datos estadísticos de una de las pocas encuestas a la población comparables de un país a otro en la sección sobre 'El panorama mundial del delito cibernético'.

3.6.3. Iniciativas de denuncia para las víctimas

Las víctimas de delito cibernético podrían a menudo preferir denunciar el acto a un centro designado para la denuncia del delito cibernético, como una página web o una línea telefónica, y no a canales policíacos tradicionales (aunque normalmente hay vínculos estrechos entre los centros de denuncia y las autoridades). Iniciativas de denuncia de este tipo existen en varios países, entre ellos, países del sur de Asia[150], Centroamérica[151], Europa Occidental[152] y Norteamérica[153]. También se encuentran cada vez más páginas para que las víctimas denuncien en varios países en desarrollo, como en África Occidental[154]. Al igual que con las estadísticas de la policía, los datos derivados de los centros de denuncia sobre delito cibernético padecen una considerable 'cifra desconocida' de eventos no denunciados. Por lo

[147] JOHNSON, H., and Nevala. S. 2010. International Violence Against Women Survey (IVAWS).

[148] http://crimevictimsurvey.eu

[149] COMISIÓN DE ESTADÍSTICA DE LAS NACIONES UNIDAS, 2012. Informe del Instituto Nacional de Estadística y Geografía de México y UNODC sobre estadísticas criminales: Hoja de ruta para mejorar la calidad y disponibilidad de estadísticas sobre delincuencia. E/CN.3/2013/11 de 19 de diciembre de 2012.

[150] Ver http://www.cybercellindia.com/#

[151] Ver http://fiscalia.chihuahua.gob.mx/intro/?page_id=3029 (México)

[152] Ver https://www.meldpuntcybercrime.nl/english_information.html; http://www.cybercrime.admin.ch/content/kobik/en/home/meldeformular.html; y http://www.actionfraud.police.uk/home

[153] Ver http://www.ic3.gov/default.aspx

[154] Ver http://cybercrime.interieur.gouv.ci/?q=node/4

tanto, a menudo no son apropiados para ser usados en comparaciones de los niveles de delito cibernético de un país a otro. Incluso las tendencias de las denuncias podrían ser impulsadas por los niveles de concientización de las víctimas, y por eventos subyacentes[155].

No obstante, las estadísticas derivadas de los mecanismos de denuncia para víctimas pueden ofrecer información sobre la distribución de los actos de delito cibernético dentro de un país particular. Las estadísticas podrían mostrar, por ejemplo, características como los principales tipos de fraude informático reportados, la distribución de la edad y el sexo de las víctimas denunciantes, o la naturaleza del contenido ilegal denunciado. Al igual que con las estadísticas registradas por la policía, la capacidad de comparar los datos de las iniciativas de denuncia para víctimas podría verse reforzada con el desarrollo de clasificaciones estandarizadas para los actos de delito cibernético.

3.6.4. Información sobre seguridad cibernética con base tecnológica

Los actos de delito cibernético son quizá únicos entre el delito en general, ya que existen medidas tecnológicas de prevención ampliamente difundidas –incluyendo productos antivirus, de seguridad para las redes y cortafuegos-[156]. El rol de dichos productos suele estar basado en escanear, identificar y filtrar ciertas 'firmas' electrónicas. Estos pueden funcionar por contenido, o por tráfico, como con las comunicaciones hacia o desde direcciones IP que estén en una 'lista negra'[157].

[155] Los informes anuales al centro de denuncia IC3 de los Estados Unidos, por ejemplo, aumentaron de manera constante desde el año 2000 a 2009 hasta que se nivelaron en 2010 y 2011.Ver Internet Crime Complaint Centre. 2011. Internet Crime Report 2011. En contraste, el número de denuncias recibidas por el centro de denuncia suizo disminuyó de 2007 a 2011. Ver Service de Coordination de la Lutte Contre la Criminalité sur Internet (SCOCI) 2011. Rapport Annuel 2011. La consciencia sobre los mecanismos de denuncia podría aumentar o disminuir con el tiempo, dependiendo de factores como el grado y consistencia de la publicidad que acompaña al mecanismo

[156]OCDE. 2002. Recomendación del Consejo con respecto a las Directrices de la OCDE para la seguridad de sistemas y redes de información - Hacia una cultura de seguridad. 25 de julio de 2002 - C(2002)131/FINAL.

[157] CALLANAN, C., Gercke, M., De Marco, E., y Dries-Ziekenheiner, H. 2009. Study on Internet blocking, balancing cybercrime responses in democratic societies. Aconite Internet Solutions, Octubre de 2009.

Muchos productos incluyen además detección heurística, que examina el comportamiento de los archivos y las conexiones sospechosas comparándolos con condiciones predeterminadas. Las bitácoras (registros) de la actividad creadas por productos tecnológicos de seguridad capturan así un subconjunto de eventos del contenido y el tráfico informático que podrían –en algunas circunstancias– corresponder a componentes de un acto de delito cibernético.

Las tentativas o los actos materializados de acceso ilegal a un sistema informático, o de interferencia ilegal de un sistema o de datos informáticos, por ejemplo, podrían ser detectados por dichos productos y que ellos mismos generen una respuesta. Una analogía vaga es la de la alarma doméstica contra ladrones que detecta eventos en las puertas y ventanas del hogar. El hecho de que se active la alarma no necesariamente quiere decir que se cometió un delito. No obstante, una cierta proporción de delitos activarán la alarma.

Una ventaja de los productos tecnológicos de seguridad cibernética es que un gran número de las 'alarmas contra ladrones' podrían reportar eventos registrados a una sede central –permitiendo la producción de estadísticas agregadas de seguridad cibernética. Muchos proveedores de seguridad cibernética del sector privado producen informes basados en esas estadísticas[158].

Sin embargo, los proveedores a menudo usan definiciones; métodos de conteo; series cronológicas; coberturas geográficas; y presentaciones de datos marcadamente distintas[159]. Como resultado, la comparación de las estadísticas de un 'informe sobre amenazas' producido por el sector privado a otro es extremadamente desafiante. En algunos casos, dichos datos son presentados como estadísticas sobre 'delito cibernético'[160]. Sin embargo, podría ser más apropiado ver

[158] AVG. 2011. Community Powered Threat Report 2012; Cisco 2011. Informe anual de seguridad Cisco 2011; IBM. 2011. IBM Informe sobre tendencias y riesgos 2011; McAfee 2012. Informe sobre amenazas de McAfee. Primer trimestre 2012; Microsoft. 2011. Informe de Inteligencia de Seguridad de Microsoft. Volumen 12; PandaLabs. 2012. Informe trimestral de PandaLabs. Abril-Junio 2012; Sophos. 2012. Informe sobre amenazas de seguridad 2012; Symantec. 2011. Informe de Amenazas a la Seguridad en Internet. Tendencias 2011, Volumen 17; Total Defense. 2011. Informe de amenazas: Final del año 2011; y Trend Micro. 2011. Informe anual sobre seguridad de TrendLabs.

[159] PricewaterhouseCoopers. 2012. Eye of the storm. Key findings from the 2012 Global State of Information Security Survey; Foro Económico Mundial. 2012. Riesgos mundiales 2012, 7a ed.

[160] Symantec. 2011. Informe de Amenazas a la Seguridad en Internet. Tendencias 2011, Volumen 17.

la información tecnológica sobre seguridad cibernética como indicativa de fenómenos de seguridad cibernética que podrían, o no, constituir actos de delito cibernético.

No obstante, se puede usar la información de los productos de seguridad cibernética sobre las 'amenazas' electrónicas, con cierta precaución, para que ayuden a comprender los patrones generales de la primera categoría del delito cibernético: los actos contra la confidencialidad, la integridad y la disponibilidad de los datos o los sistemas informáticos. Dicha información puede, en particular, ser comparable en gran medida de un país a otro, ya que es probable que el mismo producto –usando el mismo sistema de recopilación y procesamiento de datos– esté instalado en múltiples sistemas informáticos en distintos países. Este Estudio hace uso de información tecnológica sobre seguridad cibernética para caracterizar una herramienta particular, la red de bots – en inglés, botnet– que a menudo es usada en los actos de delito cibernético.

Una mayoría de los países reportaron lo inadecuado de las estadísticas policíacas para registrar actos de delito cibernético. Aunque una ligera mayoría de naciones europeas reportó que las estadísticas capturaban suficientemente los actos de delito cibernético, en todas las demás regiones, una gran mayoría de los países reportó que las estadísticas de la policía no eran suficientes para registrar esos casos.

3.7 El problema de la cifra negra

En estrecha relación con el desafío de la falta de estadísticas oficiales, se debe desarrollar la problemática de la propia falta de denuncias realizadas por las víctimas, que genera la llamada "cifra negra" de los delitos informáticos.

De acuerdo al Dr. Germán Aller[161] la cifra negra es lo más próximo numéricamente a la cantidad real de crímenes cometidos en una sociedad determinada. La relación de tensión existente entre delitos realmente cometidos y

[161] ALLER, Germán. "Cuestiones Victimológicas de Actualidad: Origen de la Victimología, Seguridad, Cifra Negra, Personalización del Conflicto y Proceso Penal". Revista ILANUD Nro. 27, 2006.

los efectivamente tratados por el aparato penal, engloba a la mayor cantidad de víctimas que ni siquiera serán atendidas, tratadas ni conocidas por el segmento penal, y a las cuales el Estado no da respuesta alguna. De acuerdo a Aller, tal proceso "empuja" a las personas a no denunciar los actos ilícitos, a no reconocerse a sí mismas como víctimas y, en consecuencia, a la impunidad que el infractor penal asume, puesto que en el acto desvalorado no vislumbra un referente social acompasado del penal, en tanto a su conducta es delictiva, pero el núcleo social o persona menoscabada por el delito que se ha cometido no pone en evidencia tal daño, y por ende, tampoco el segmento penal podrá operar en su contra.

De acuerdo a este autor, muchas víctimas no denuncian los delitos sufridos porque:

1) No se cree en la Policía ni en la Justicia Penal.

2) No se acepta la condición de víctima, debido a que implica pérdida de dignidad y falta de solidaridad.

3) No se quiere evidenciar la victimización individual ni colectiva.

4) El aparato penal carece de plataforma adecuada para abordar ni siquiera con un mínimo de éxito la solución del conflicto social base.

5) Se tiene miedo a la venganza o amenazas posteriores por parte del autor del delito.

6) Se quiere olvidar lo ocurrido.

7) Se desconoce que se haya cometido un delito.

8) La víctima se siente total o parcialmente culpable de lo sucedido.

9) Se ignora que puede pedir la intervención del Estado.

A simple vista, se pueden reconocer en el listado de causas realizado por el Dr. Aller, varios aplicables al ámbito del cibercrimen. Puntualmente, se tomarán algunas de ellas, con el objetivo de un desarrollo personal sobre dichos aspectos.

a) Falta de confianza en la Policía o la Justicia: En nuestro país este aspecto es relevante en la mayoría de los casos, ya que existe un alto porcentaje de

la población que tiene falta de confianza en la Justicia. Así lo demuestran desde hace años los estudios del Índice de Confianza en la Justicia[162] (ICJ) realizados por Fores, la Escuela de Derecho de la Universidad Torcuato Di Tella, y la Fundación Libertad. A Marzo de 2010, los índices de confianza fueron del 50,5% (en una escala donde 0 expresa el mínimo de confianza y 100 el máximo). El mismo estudio revela, por ejemplo, que "En términos de eficiencia... la Justicia en Argentina es..." poco confiable para el 55% de los encuestados, y nada confiable para el 22% de la población consultada.

b) El aparato penal carece de plataforma adecuada para abordar ni siquiera con un mínimo de éxito la solución del conflicto social base: Este punto, si bien tiene estrecha relación con el anterior, reviste sus diferencias. Puntualmente, es menester destacar que en muchos casos de delitos informáticos, para poder realizar una investigación eficaz tendiente a determinar y capturar al autor del mismo, es necesario poseer una infraestructura adecuada. Es decir, se precisa contar con los recursos técnicos necesarios, con personal disponible y capacitado, así como cierta agilidad en cuanto a coordinación y cooperación de distintos entes (relación ISP / Justicia). Todos estos aspectos no suele encontrarse (salvo excepciones) a lo largo de nuestro país, radicando aquí otra de las grandes problemáticas a ser abordadas.

c) Se desconoce que se haya cometido un delito: Desde la experiencia en el trabajo privado de consultoría en seguridad informática, se puede afirmar que muchas personas que escriben para consultar por los problemas que han tenido en Internet, desconocen totalmente que han sido víctimas de un delito informático tipificado en Argentina. Esta falta de conocimiento por parte del promedio de la sociedad sobre la existencia de estos "novedosos" delitos, hace que varios casos se pierdan dentro de la gran bolsa de la cifra negra.

Antes de finalizar en este punto, consideramos oportuno agregar un elemento nuevo, o al menos una causa no considerada por el Dr. Aller, que desde la

[162] FORO DE ESTUDIOS SOBRE LA ADMINISTRACIÓN DE JUSTICIA, "Indice de Confianza en la Justicia". http://j.mp/1rE9SiB Consultado: 27 de Noviembre de 2013

experiencia se puede afirmar que es un aspecto decididamente relevante al momento de analizar la falta de denuncias sobre casos vinculados al cibercrimen.

d) Confidencialidad como requisito: Muchas víctimas de distintos tipos de delitos informáticos deciden voluntariamente no denunciar sus casos, bajo el razonamiento que la posibilidad de difusión pública ocasionaría un daño peor al ya efectivamente sufrido. En este sentido, dentro del ámbito privado de la seguridad informática, una de las principales virtudes que analizará un cliente, será precisamente el nivel de profesionalismo en relación a la confidencialidad de los casos. Dicha situación encuentra una lógica respuesta considerando que la víctima es consciente que de difundirse públicamente el incidente que ha sufrido (algo potencialmente probable en caso de denuncia ante las autoridades), las consecuencias hacia su imagen, buen nombre, reputación, etc., puede ser gravemente perjudicada, superando ampliamente el daño ya recibido por el ataque informático en sí mismo.

A modo de mejorar el sentido de este aspecto, se citan dos ejemplos para la facilidad de comprensión de los lectores. Supongamos el caso de una importante empresa dedicada al rubro de la salud (clínica por ejemplo), la cual es víctima de ataques informáticos que logran acceder a sus sistemas y hacerse con todas sus bases de datos, las cuales poseen información sensible sobre la salud de miles de personas de la región. La difusión de dicho incidente podría ocasionar daños irreparables en cuanto a la confianza de los clientes, construida en base al trabajo de muchos años. Otro ejemplo puede ser el caso de un profesional reconocido en su ambiente (un periodista, un abogado, un psicólogo) el cuál es víctima de un caso de interceptación de comunicaciones electrónicas (cuentas “pinchadas”), permitiendo que terceros extraños accedan a todas sus comunicaciones privadas (y eventualmente difundidas). Fácilmente puede advertirse que los daños ocasionados por una noticia (que vale destacar que son generalmente buscadas atendiendo a la gran recepción que existe en la masa sobre este tipo de casos de problemas “cibernéticos”) pueden ocasionar perjuicios irreparables, afectándose bienes jurídicos de difícil reconstrucción (como la imagen, honor o reputación de una

persona física o jurídica), comparativamente mucho más graves al daño ya sufrido por el delincuente informático.

3.7.1 Estadísticas del Proyecto ODILA

El Proyecto ODILA (Observatorio Latinoamericano de Delitos Informáticos) es un proyecto conjunto, llevado adelante por el Lic. Cristian Borghello (Segu-Info), el A.I.A. Maximiliano Macedo (AsegurarTe) y el autor de la presente tesis, que ha funcionado desde el año 2015 al 2022.

Este proyecto buscó construir un espacio de investigación, encuentro y trabajo sobre la realidad latinoamericana en materia de delitos informáticos y cibercrimen, especialmente dedicado a relevar información sobre incidentes o delitos informáticos ocurridos en los países de Latinoamérica.

En los últimos reportes realizados[163] por este Observatorio, se han publicado los siguientes resultados que consideramos pertinentes para este estudio.

163 ODILA: https://odila.org/reporte

¿Ha denunciado?

ODILA Observatorio de Delitos Informáticos de Latinoamérica



¿Ha Denunciado?	No, no denuncié porque... (ver siguiente pregunta)	Si, ya denuncie y la investigación está en curso	Si, denuncie pero la investigación no avanzó	Sí, denuncié y ya se ha condenado al o los culpables.
Porcentaje	83,82 %	9,83 %	0,35 %	6,00 %

Entre los datos más importantes de ODILA se encuentra el indicador sobre si el usuario ha realizado la denuncia formal sobre el hecho del cuál ha sido víctima. Es precisamente este indicador el que nos permite observar de forma directa el nivel de la cifra negra, es decir, la cantidad de delitos que realmente ocurren pero que no son tratados ni conocidos por el segmento penal y, en consecuencia, a los cuales el Estado no tiene siquiera la posibilidad de dar respuesta alguna.

Destacamos uno de los números más importantes del estudio, ya que en un 83,82% las personas que reportaron el incidente, afirmaron que no han realizado la denuncia formal ante los organismos competentes. Es decir, que podemos afirmar que 8 de cada 10 delitos informáticos no son denunciados formalmente por parte de las propias víctimas y, por lo tanto, no tienen ningún tipo de consecuencia penal.

Por otro lado, un 9,83% de los usuarios, ha reconocido haber hecho la denuncia formal y afirma que la investigación del hecho se encuentra en curso. En cambio, el 0,35% restante que ha denunciado formalmente el hecho, dice que la investigación no avanzó (por distintos motivos).

Finalmente, un 6% declara haber realizado la denuncia formal, afirma que la investigación ha finalizado y se ha logrado conseguir una condena efectiva sobre el imputado. Es decir, de cada 100 delitos informáticos, sólo 6 lograría llegar a obtener condena efectiva (sin tener en consideración el tipo de condena lograda).

En relación a la interpretación de estas cifras, cabría hacer una consideración en relación a los usuarios y, por lo tanto, a la información recolectada: es posible que una importante cantidad de los usuarios del Observatorio que completan las encuestas, sean aquellos que están en la etapa de "búsqueda de información", es decir, aquellas víctimas de algún incidente de seguridad de la información que no saben si han sido víctima de un delito informático en particular, o dónde debe dirigirse para denunciarlo, por ejemplo.

Por lo tanto, si los usuarios se encuentran en esta etapa, lo más probable es que afirman que aún no han realizado sus respectivas denuncias ante los organismos competentes. De hecho, ODILA pretende ser efectivamente una fuente de información para que los usuarios identifiquen si han sido víctimas, se informen sobre las dependencias estatales habilitadas y puedan ir a realizar allí sus denuncias.

Esta interpretación, parte de la presunción que muchos de los usuarios del Observatorio, llegan al mismo a través de búsquedas voluntarias en Internet, intentando obtener información que les brinde una guía acerca de qué deberían hacer, o cuáles serían los pasos a seguir para denunciar un delito informático.

Para poder explicarlo de otra manera, es posible que quien ya haya realizado una denuncia formal, esté menos interesado en buscar información y, por lo tanto, en utilizar y aportar datos en ODILA.

En las tablas comparativas, donde se exhiben los resultados parciales de los distintos cortes realizados, nos permiten arribar a una serie de conclusiones extras sobre esta categoría.

Tablas comparativa

ODILA Observatorio de Delitos Informáticos de Latinoamérica

¿Ha denunciado?

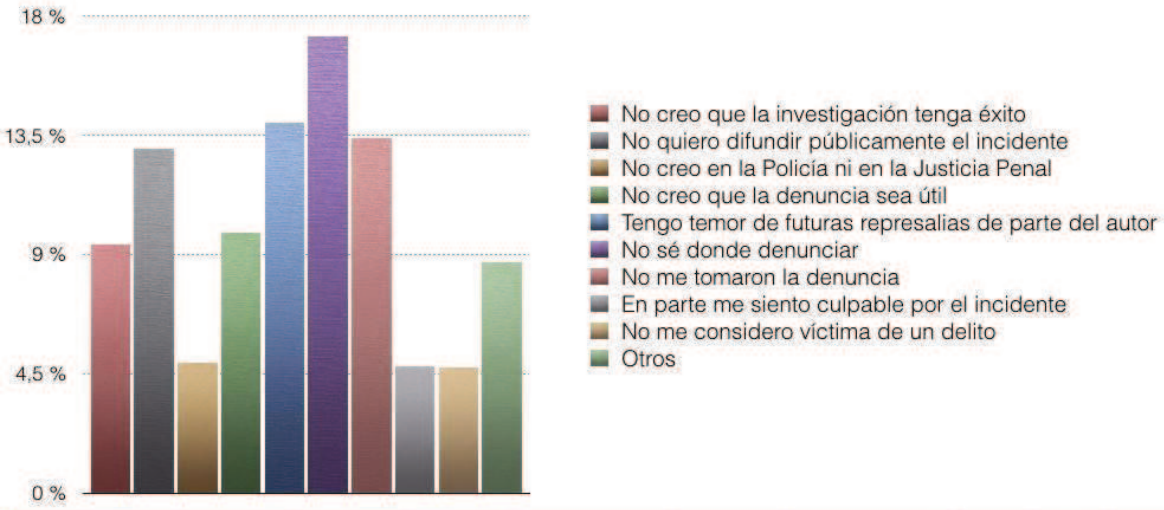
¿Ha Denunciado?	No, no denuncié porque...	Si, ya denuncie y la investigación está en curso	Si, denuncie pero la investigación no avanzó	Sí, denuncié y ya se ha condenado al o los culpables.
Porcentaje 2014-2015	68,22 %	16,28 %	15,5 %	0 %
Porcentaje 2015-2016	82,54 %	5,56 %	11,11 %	0,79 %
Porcentaje 2016-2017	83,67 %	6,12 %	9,18 %	1,02 %
Promedio 2014-2017	78,14 %	9,32 %	11,93 %	0,60 %
Porcentaje Histórico 2014-2022	83,82 %	9,83 %	0,35 %	6,00 %
Diferencia Histórico vs. Promedio 2017	5,68 %	0,51 %	-11,58 %	5,39 %

De la tabla comparativa de los distintos cortes podemos extraer que con el paso de los años, han pasado diversas cosas. Por un lado, puede observarse que el nivel de la cifra negra, excepto por el primer período, siempre osciló por encima del 80%, dando un promedio histórico de casi un 84%.

Por otro lado, podemos ver que en un comienzo, el porcentaje de denuncias con investigaciones en curso era más alto, y con el pasar de los años fue decreciendo. A su vez, y como un dato más alentador, podemos observar que con el paso de los años, se fue incrementando las denuncias con condenas efectiva (incrementándose mucho más en los últimos 4 años), llegando a un máximo del 6%. Este contexto, a su vez, es coherente con el decrecimiento de aquellas denuncias realizadas pero cuyas investigaciones no han avanzado o se han estancado.

Causas de la no denuncia

ODILA Observatorio de Delitos Informáticos de Latinoamérica



Causas	No creo que la investigación tenga éxito	No quiero difundir públicamente el incidente	No creo en la Policía ni en la Justicia Penal	No creo que la denuncia sea útil	Tengo temor de futuras represalias de parte del autor	No sé donde denunciar	No me tomaron la denuncia	En parte me siento culpable por el incidente	No me considero víctima de un delito	Otros
%	9,39 %	13,01 %	4,91 %	9,84 %	13,99 %	17,25 %	13,39 %	4,79 %	4,74 %	8,70 %

Entre las distintas causas por las cuáles no ha denunciado, se desprenden como los valores más importantes a destacar que el 17,25% no denuncia porque no sabe donde denunciar, quedando en evidencia uno de los aspectos más problemáticos que ODILA intenta combatir: la falta de información. Este índice, implica que la víctima está dispuesta a realizar la denuncia, pero que no encuentran en el Estado (del país que corresponda) una respuesta adecuada en cuanto a brindarle información oficial, o bien en un centro de respuesta o de atención a las víctimas de la ciberdelincuencia. Independientemente del organismo u oficina que se trate, cabe destacar la importancia que debería tener el acceso real para las víctimas.

En segundo lugar, con un 14% de las víctimas, no denuncia porque tiene temor a futuras represalias por parte del autor del delito, evidenciando que la víctima continúa o tiene la sensación de que puede volver a ser nuevamente víctima del ataque por parte del mismo ciberdelincuente (aspecto analizado en el punto 4.7.5)

En tercer lugar, el 13,4% de las víctimas sostienen que intentaron realizar la denuncia pero que el organismo público al cual asistieron, no le han recibido la misma, exhibiendo una clara falta por parte del Estado en la obligación de recepcionar las denuncias, para recién en un paso posterior considerar si el hecho denunciado puede ser calificado o no como un delito de acuerdo al sistema penal vigente de dicho lugar.

En cuarto lugar, aparece la falta de confidencialidad como causa, dado que un 13% de las víctimas no quiere realizar la denuncia por temor a que se difunda públicamente el hecho sufrido (aspecto analizado en el punto 4.7.10). Es decir, el sistema no ofrece las condiciones de privacidad o confidencialidad para resguardar el nombre, honor o imagen de la víctima, ya sea una persona física o jurídica.

Muchas víctimas de distintos tipos de delitos informáticos deciden voluntariamente no denunciar sus casos, bajo el razonamiento que la posibilidad de difusión pública ocasiona un daño peor al ya efectivamente sufrido. Es decir, las personas priorizan el requisito de la confidencialidad por sobre la necesidad de que dicho incidente sea investigado penalmente por las autoridades competentes.

En el caso de las organizaciones, este hecho también está asociado a que la exposición del incidente implicaría el reconocimiento público de haber sufrido el problema de seguridad, revelando la falta de medidas al respecto en algún caso, y generando sobre todo, pérdidas de imagen sobre la organización. La difusión de la noticia sobre el incidente rápidamente podría transformarse en un perjuicio mayor para la víctima.

En quinto lugar, con 9,84%, las víctimas reconocen no realizar la denuncia por considerar que no creen que la misma sea útil, es decir, que consideran que el aparato penal carece de plataforma adecuada para abordar ni siquiera con un mínimo de éxito la solución del conflicto social base (aspecto analizado en el punto 4.7.4.). Esta causa no se refiere a la falta de confianza hacia la justicia como servicio a la sociedad, que es otra de las opciones que se pueden seleccionar, sino una falta de expectativa a que la denuncia del delito sirva para lograr un cambio sobre el conflicto social base, incluso teniendo la posibilidad de llegar a una condena para el delincuente.

En sexto lugar, con un 9,39%, las víctimas reconocen que su no denuncia tiene como fundamento la falta de confianza acerca de que el sistema penal pueda, con un mínimo de eficacia, tomar su caso e investigarlo con éxito, es decir, falta de confianza en la justicia como servicio que brinda su propio Estado (aspecto analizado en el punto 4.7.1)

Es interesante analizar que casi un 5% de las personas dicen que no se consideran víctimas y, en razón de ello, deciden no realizar la denuncia formal. Este dato podría ser analizado también por la falta de información por parte de los usuarios, ya que en general existe una situación de duda sobre si lo que están sufriendo configura o no un delito penal en el país donde se encuentran.

En las tablas comparativas, donde se exhiben los resultados parciales de los distintos cortes realizados, nos permiten arribar a una serie de conclusiones extras sobre esta categoría.

Tabla comparativa

ODILA Observatorio de Delitos Informáticos de Latinoamérica

Causas de no denuncia

Causas	No creo que la investigación tenga éxito	No quiero difundir públicamente el incidente	No creo en la Policía ni en la Justicia Penal	No creo que la denuncia sea útil, porque el sistema penal	Tengo temor de futuras represalias de parte del autor	No sé donde denunciar	No me tomaron la denuncia	En parte me siento culpable por el incidente	No me considero víctima de un delito	Otros
Porcentaje 2014-2015	17,00 %	17,00 %	12,00 %	12,00 %	10,00 %	9,00 %	7,00 %	7,00 %	5,00 %	4,00 %
Porcentaje 2015-2016	16,19 %	12,38 %	8,57 %	5,71 %	16,19 %	19,05 %	4,76 %	0,95 %	13,33 %	2,86 %
Porcentaje 2016-2017	14,05 %	16,12 %	9,09 %	16,94 %	14,05 %	14,88 %	2,07 %	3,31 %	6,20 %	3,31 %
Promedio 2014-2017	15,75 %	15,17 %	9,89 %	11,55 %	13,41 %	14,31 %	4,61 %	3,75 %	8,18 %	3,39 %
Porcentaje Histórico 2014-2022	9,39 %	13,01 %	4,91 %	9,84 %	13,99 %	17,25 %	13,39 %	4,79 %	4,74 %	8,70 %
Diferencia Histórico vs. Promedio 2017	-6,36 %	-2,16 %	-4,98 %	-1,71 %	0,57 %	2,94 %	8,78 %	1,04 %	-3,44 %	5,31 %

Pregunta no obligatoria, y de selección múltiple

Del análisis de la tabla comparativa pueden extraerse algunas conclusiones extras, tales como a medida que fueron pasando los años, las víctimas continuaron

con un alto índice de no denuncia por falta de información (como no saber donde denunciar).

También es posible observar que la falta de toma de las denuncias no era una de las causas principales de la no denuncia, pero sin embargo es algo que creció mucho en la última etapa de 2017 a 2022 (con posible afectación del efecto pandémico).

También es posible observar que la falta de confianza sobre que la investigación éxito siempre estuvo en los primeros lugares de las causas de la no denuncia, de la misma forma que el interés de la víctima en mantener la confidencialidad del hecho sufrido.



Incidente	Calumnias o Injurias	Violación de Datos Personales	Amenazas	Fraude o Estafa Informática	Hacking	Suplantación de identidad digital	Pornografía Infantil	Grooming	Phishing	Cracking	Difusión de Malware	Denegación de Servicio
Porcentaje	20,02 %	17,02 %	16,49 %	8,82 %	8,77 %	8,47 %	6,57 %	5,03 %	4,37 %	2,07 %	1,50 %	0,88 %

De acuerdo a los resultados históricos obtenidos, podemos observar que en primer lugar (con 20,02%) encontramos a las calumnias a través de las TICs, uno de los delitos más comunes que se ha vuelto cada vez más grave (con distintos niveles de daño al honor y reputación de las personas).

La utilización masiva de las redes sociales, combinada con la sensación de "impunidad" y la exacerbación de la libertad de expresión, podrían determinar el crecimiento de esta actividad delictiva. Como apreciación adicional, en muchos casos las víctimas consideran que los dichos (a través de medios electrónicos) de una persona (determinada o indeterminada) son lo suficientemente graves como para calificar y ser considerados como injurias o calumnias. Dicha apreciación de las víctimas, posteriormente debe ser analizada por el fiscal o autoridad correspondiente, que deberá realizar un análisis de ponderación sobre la viabilidad del caso.

En segundo lugar encontramos a la violación de datos personales como delito más denunciado, entendiendo que el mismo puede incluir tanto el acceso indebido a datos personales, así como también, el tratamiento no autorizado (como venta ilegal) de dichos datos, tipificados en los distintos países desarrollados anteriormente. La problemática sobre la violación de los datos personales es algo cada vez más preocupante, donde cada vez existen mayores casos de grandes empresas u organismos que son atacadas y filtradas sus bases de datos (sólo en Argentina, podemos citar como caso de RENAPER[164])

En tercer lugar encontramos que las amenazas a través de medios electrónicos han sido el problema más reportado por los usuarios (16,49%). Con respecto a este delito en particular, debemos mencionar que es posible que el incremento de herramientas y medidas que permiten brindar un alto nivel de anonimato para el emisor de una comunicación electrónica, terminen dando como consecuencia un incremento en este tipo de delitos. Adicionalmente es necesario mencionar, que cabe realizar un análisis particular sobre cada uno de los casos (tarea que excede a las misiones del Observatorio) para poder conocer si realmente se encuentran dados todos los elementos jurídicos que se necesitan para que pueda ser realmente considerado como amenaza.

También esbozamos como hipótesis que el incremento de este tipo de denuncia, puede haberse visto afectado por el crecimiento masivo de los casos de

[164] Diario El Economista; "Hackean RENAPER: habló el hacker y asegura tener copia de los datos, planea venderlos y filtrarlos"; Url: https://eleconomista.com.ar/tech/hackean-renaper-hablo-hacker-asegura-tener-copia-datos-planea-venderlos-filtrarlos-n47003

ransomware en el mundo (fenómeno de Wanancry en mayo y NotPetya en julio de 2017). Entre los tipos penales disponibles por ODILA, no se encuentra aún disponible alguno dedicado a este tipo particular de incidente informático; por lo cual es posible que los usuarios víctimas del mismo, hayan seleccionado la opción "amenazas", entendiéndolo como sinónimo de "extorsión".

En cuarto lugar, encontramos a los fraudes y estafas informática (8,82%) que, durante estos tres años del Observatorio, siempre han estado dentro del ranking de los cinco delitos más reportados. Las estafas y fraudes a través de medios electrónicos no dejan de seguir estando vigentes, porque terminan siendo para los delincuentes, la forma más sencilla y directa de acceder a un beneficio económico.

En las tablas comparativas, donde se exhiben los resultados parciales de los distintos cortes realizados, nos permiten arribar a una serie de conclusiones extras sobre esta categoría.

Tabla comparativa

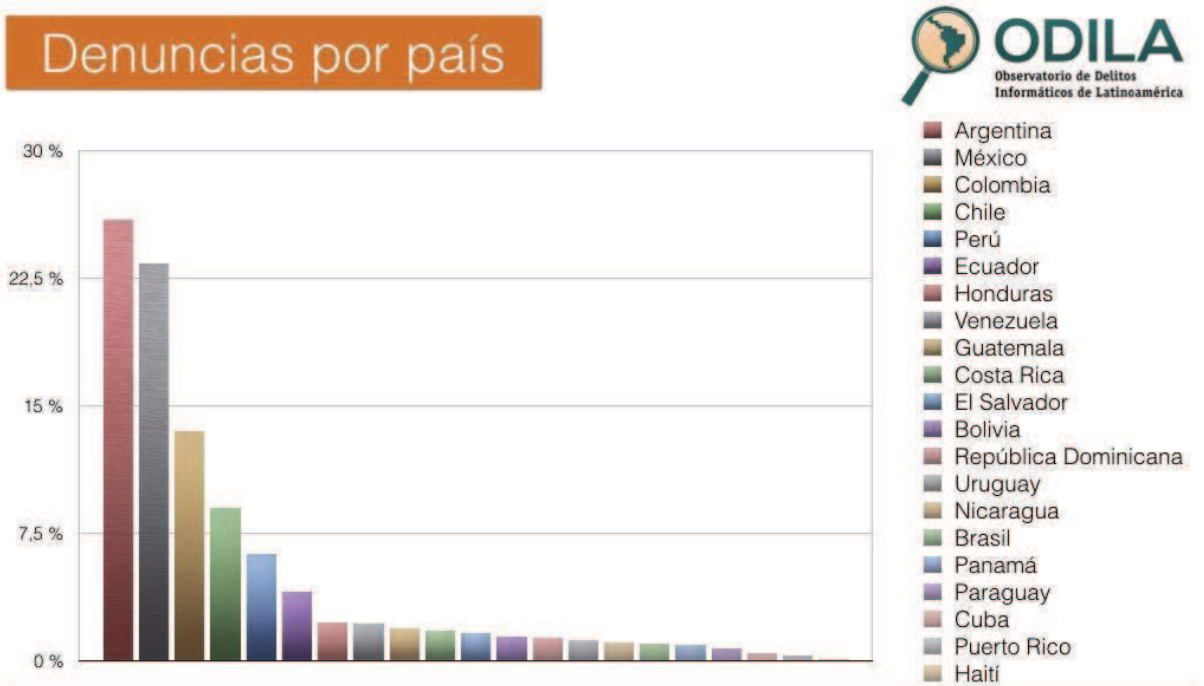
ODILA Observatorio de Delitos Informáticos de Latinoamérica

Delitos denunciados

Incidente	Hacking	Calumnias o Injurias	Suplantación de Identidad	Amenazas	Fraude o Estafa Informática	Cracking	Phishing	Violación de Datos Personales	Grooming	Difusión de Malware	Denegación de Servicio	Pornografía Infantil
Porcentaje 2014-2015	22,48 %	17,05 %	9,3 %	8,53 %	8,53 %	7,75 %	7,75 %	7,75 %	3,88 %	3,1 %	1,55 %	1,55 %
Porcentaje 2015-2016	13,49 %	11,11 %	11,11 %	9,52 %	12,70 %	8,73 %	9,52 %	7,94 %	1,59 %	4,76 %	3,17 %	6,35 %
Porcentaje 2016-2017	7,65 %	14,80 %	9,18 %	17,35 %	12,24 %	3,06 %	10,71 %	11,22 %	5,10 %	3,06 %	2,04 %	3,57 %
Promedio 2014-2017	14,54 %	14,32 %	9,86 %	11,80 %	11,16 %	6,51 %	9,33 %	8,97 %	3,52 %	3,64 %	2,25 %	3,82 %
Porcentaje Histórico 2014-2022	8,77 %	20,02 %	8,47 %	16,49 %	8,82 %	2,07 %	4,37 %	17,02 %	5,03 %	1,50 %	0,88 %	6,57 %
Diferencia Histórico vs. Promedio 2017	-5,77 %	5,70 %	-1,40 %	4,69 %	-2,34 %	-4,44 %	-4,96 %	8,05 %	1,50 %	-2,14 %	-1,37 %	2,75 %

De acuerdo a la tabla comparativa expuesta, podemos hacer algunas consideraciones adicionales:

- Que, el delito de acceso indebido a sistemas informáticos (hacking) comenzó siendo uno de los más denunciados y con el paso de los años fue bajando notablemente.
- Que, los delitos de calumnias e injurias por internet, así como el fraude o estafa informática siempre han tenido una tasa alta de reportes en el Observatorio, estando siempre entre los primeros puestos.
- Que el delito de violación de datos personales, comenzó sin ser uno de los principales delitos y con el correr de los años, fue creciendo cada vez más.



País	Ar	Mx	Co	Ch	Pe	Ec	Hn	Ve	Gt	Cr	Sv	Bo	Do	Uy	Ni	Br	Pa	Py	Cu	Pr	Ht
%	25,93 %	23,37 %	13,45 %	8,95 %	6,26 %	4,06 %	2,25 %	2,16 %	1,85 %	1,76 %	1,63 %	1,37 %	1,32 %	1,19 %	1,01 %	0,97 %	0,93 %	0,71 %	0,44 %	0,31 %	0,09 %

En relación a la cantidad de denuncias por país, se observa que en su gran mayoría los reportes han sido realizados en Argentina (25,93%), en estrecha relación con que los medios de difusión a los cuáles se ha tenido alcance desde el observatorio, sólo han podido ser canales de alcance nacional, considerando que el proyecto es gestionado desde Argentina, con casi nula difusión internacional (sólo a través de redes sociales).

Tabla comparativa

ODILA Observatorio de Delitos Informáticos de Latinoamérica

Denuncia por países

País	Ar	Mx	Co	Br	Ve	Bo	Pe	Ch	Gt	Hn	Pa	Ni	Cr	Cu	Ht	Py	Pr	Do	Ec	Sv	Uy
% 2014 al 2015	51,94 %	10,65 %	6,2 %	5,43 %	3,88 %	3,1 %	3,1 %	2,33 %	2,33 %	2,33 %	2,33 %	1,55 %	0,78 %	0,78 %	0,78 %	0,78 %	0,78 %	1,59 %	0 %	0 %	0 %
% 2015 al 2016	54,76 %	4,76 %	8,73 %	0,79 %	1,59 %	2,38 %	2,38 %	0,79 %	3,17 %	7,94 %	0,79 %	0,79 %	0,79 %	0 %	0,79 %	0 %	0,79 %	0,79 %	4,76 %	0 %	2,38 %
% 2016 al 2017	41,33 %	17,86 %	11,22 %	1,02 %	2,55 %	1,02 %	6,12 %	4,59 %	5,10 %	2,04 %	0,51 %	1,02 %	1,02 %	0,00 %	0,00 %	0,51 %	0,00 %	0,00 %	2,04 %	1,02 %	1,02 %
% 2014-2017	49,34 %	11,16 %	8,72 %	2,41 %	2,67 %	2,17 %	3,87 %	2,57 %	3,53 %	4,10 %	1,21 %	1,12 %	0,86 %	0,26 %	0,52 %	0,43 %	0,52 %	0,79 %	2,27 %	0,34 %	1,13 %
% 2014-2022	25,93 %	23,37 %	13,45 %	0,97 %	2,16 %	1,37 %	6,26 %	8,95 %	1,85 %	2,25 %	0,93 %	1,01 %	1,76 %	0,44 %	0,09 %	0,71 %	0,31 %	1,32 %	4,06 %	1,63 %	1,19 %
2017 vs Histórico	(23,41 %)	12,21 %	4,73 %	(1,44 %)	(0,51 %)	(0,80 %)	2,39 %	6,38 %	(1,68 %)	(1,85 %)	(0,28 %)	(0,11 %)	0,90 %	0,18 %	(0,43 %)	0,28 %	(0,21 %)	0,53 %	1,79 %	1,29 %	0,06 %

En segundo lugar, podemos observar a México (23,37%), que como podemos observar en la tabla comparativa, comenzó con mucha menos participación y con el paso de los años fue utilizándose cada vez más en dicho país.

En tercer lugar, se encuentra Colombia (13,45%) , que también siempre ha sido el tercer país con más reportes, pero que al igual que México, en los últimos 5 años, su participación fue creciendo notablemente.

Capítulo IV: La tipificación de los delitos informáticos

4.1. Introducción

Manuel Castells[165], en ocasión de un discurso del 2001, y hablando del "caos" positivo que Internet genera en la comunicación, dijo: "*Técnicamente, Internet es una arquitectura de libertad. Socialmente, sus usuarios pueden ser reprimidos y vigilados mediante Internet. Pero, para ello, los censores tienen que identificar a los transgresores, lo cual implica la definición de la trasgresión y la existencia de técnicas de vigilancia eficaces. La definición de la trasgresión depende, naturalmente, de los sistemas legales y políticos de cada jurisdicción. Y aquí empiezan los problemas. Lo que es subversivo en Singapur no necesariamente lo es en España*". Al terminar dicha frase citó el ejemplo de cuando en 2000 un sitio Web de EE.UU. organizó la venta de votos de personas ausentes, hecho que representaba un delito electoral en ese país. Pero la Web se mudó a Alemania, donde ese hecho ya no podía ser perseguido por las leyes de ese país.

En consecuencia, como hemos repasado al momento de analizar la transnacionalidad de estos delitos, observamos que uno de los desafíos que tiene el derecho es la persecución de delincuentes informáticos que organizan sus ataques desde lugares con poca o nula legislación en la materia, o bien, en aquellos países que aún teniendo legislación al respecto, no poseen un adecuado sistema para la detección y persecución eficaz de este tipo de delitos.

Un ejemplo concreto de ello fue el caso de un ataque de tipo viral que costó a empresas norteamericanas miles de millones de dólares, el cuál fue atribuido por el FBI a un estudiante en Filipinas al que no se lo pudo acusar de crimen alguno.

[165] CASTELLS; Manuel, "Internet, libertad y sociedad: una perspectiva analítica", Conferencia inaugural del curso académico 2001-2002 de la UOC.

Rápidamente el gobierno filipino dispuso legislación para combatir el crimen cibernético con el objetivo de evitar futuros inconvenientes.[166]

Como hemos observado en el capítulo anterior, en un contexto de incremento de la ciberdelincuencia organizada a nivel mundial, los llamados "paraísos legales informáticos", terminan siendo considerados como potenciales bases operativas al momento de ejecución de sus actividades criminales.

En palabras de una voz autorizada, como la del Dr. Marcelo Riquert[167], "*habida cuenta de las posibilidades que brindan las nuevas tecnologías de la comunicación y la aparición en escena de un nuevo espacio, el virtual o ciberespacio, en materia de delincuencia, facilitando la afectación de bienes jurídicos a una distancia y con una velocidad impensadas, resulta un lugar común la afirmación de estar en presencia de una problemática frente a la que el proceso de homogeneización legislativa y de cooperación en los ámbitos sustantivos y adjetivos, es una necesidad ineludible si se quiere evitar la existencia de "paraísos" de impunidad*".

Es decir, como reflejan los autores citados, la transnacionalidad como característica tiene consecuencias en el aumento de la criminalidad informática por un lado, y dificulta la investigación de los propios delitos por otro.

En el marco de todo lo expuesto, una de las tareas programadas en la presente investigación consiste en realizar un análisis sobre la situación de los delitos informáticos en su aspecto material sustantivo, a través de un desarrollo de derecho comparado sobre los diferentes países alcanzados en este estudio.

A través de este análisis se busca por un lado comprobar la situación sobre la homogeneización legislativa a nivel lationamericano (limitada a los países alcanzados), y por otro, comparar la situación de dichos países en relación a dos instrumentos internacionales que de un modo u otro tienen por destino buscar esa homogeneización a nivel mundial.

---

[166] WILLIAMS, Phil, "Organized Crime and Cybercrime: Synergies, Trends, and Responses", International Information Programs, Electronic Journal of the U.S. Department of State – August 2001 Volume 6, Number 2.

[167] RIQUERT, Marcelo Alfredo, "Estado de la Legislación contra la Delincuencia Informática en el Mercosur" (en línea), URL: http://www.pensamientopenal.com.ar/node/ 27142 Consulta: 25/07/13

4.2. Estudios realizados por la ONUDC

En la búsqueda de estudios que brinden datos sobre la problemática objeto de nuestra tesis, y desde una óptica más internacional, es posible citar el *Comprehensive Study on Cybercrime*[168] -o estudio exhaustivo sobre cibercrimen- realizado por Naciones Unidas-, en particular por la United Nations Office on Drugs and Crime (ONUDC), publicado en Febrero de 2013 y en el cuál se encuestaron más de 82 países, incluyendo varios de Latinoamérica (entre ellos, Argentina).

Para la recopilación de información, la ONUDC elaboró un cuestionario que fue difundido entre los Estados Miembros, las organizaciones intergubernamentales y las entidades del sector privado. Además, teniendo en cuenta la necesidad de equilibrar la representación de las diferentes regiones, se consultó a los representantes del sector privado, incluidos los representantes de los proveedores de servicios de Internet, los usuarios de los servicios y otros actores pertinentes; así como a representantes del mundo académico, tanto de los países desarrollados y en desarrollo.

Se afirma en este instrumento que las medidas jurídicas tienen un rol clave en la prevención y la lucha contra el delito cibernético, entendiendo que se requieren medidas de este tipo en todas las áreas, incluyendo la tipificación, los poderes procesales, jurisdicción, la cooperación internacional y la responsabilidad de los proveedores de servicios de Internet, es decir, avanzar sobre un alcance más integral (y no solamente sobre el aspecto penal material).

El estudio trabaja sobre la idea que tanto las leyes existentes como las nuevas sobre delito cibernético (o las previstas), suelen estar relacionadas con la criminalización -parte de la hipótesis de nuestra tesis-, lo cual indica un interés predominante en establecer figuras delictivas específicas para los principales actos del delito cibernético. Sin embargo, los países cada vez reconocen más la necesidad de legislar en otras áreas.

[168] NACIONES UNIDAS, New York, 2013. UNODC. Comprehensive Study on Cybercrimen. Url: http://www.unodc.org/documents/organizedcrime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf. Consultado: 27 de Noviembre de 2019

Según el estudio, en comparación con las leyes existentes sobre delito cibernético, las nuevas o las que están siendo planificadas suelen abordar con mayor frecuencia las medidas investigativas, la jurisdicción, la evidencia electrónica y la cooperación internacional. Esta última afirmación, servirá de punto de comparación con los resultados parciales de esta primera parte de la tesis.

Según este estudio (recordemos que fue realizado en 2013), a nivel mundial menos de la mitad de los países encuestados perciben que sus marcos legales en materia penal y procesal sean suficientes, aunque esto oculta enormes diferencias regionales. Mientras que más de dos tercios de los países de Europa reportan legislación suficiente, el panorama se invierte en África, en las Américas, Asia y Oceanía, donde más de dos tercios de los países consideran sus leyes parcialmente suficientes o de plano insuficientes. Solo la mitad de los países que reportaron que sus leyes eran insuficientes señalaron también leyes nuevas o planificadas, destacando así una necesidad urgente de fortalecer las disposiciones legislativas en estas regiones.

A nivel normativo, el estudio recopiló la información sobre las leyes penales sobre delito cibernético a través del cuestionario del estudio, y del análisis de fuentes primarias de la legislación disponible recogida por la Secretaría[169]. El cuestionario del estudio hacía referencia a 14 actos comúnmente incluidos en el concepto de delito cibernético[170].

Los países encuestados describieron una amplia tipificación de estos 14 actos, con la excepción, principalmente, de los delitos relativos al correo basura y, en menor medida, de los delitos relacionados con el uso indebido de los dispositivos informáticos, el racismo y la xenofobia, y la intimidación u 'acoso' (grooming) de menores en línea.

[169] Se analizaron las fuentes primarias de la legislación de 97 Estados Miembro, incluidos 56 que respondieron al cuestionario con la siguiente distribución regional: África (15), América (22), Asia (24), Europa (30) y Oceanía (6)

[170] Acceso ilícito a un sistema informático; acceso ilícito, intercepción o adquisición de datos informáticos; interferencia ilegal de datos o interferencia de sistemas; producción, distribución o posesión de herramientas para el uso indebido de las computadoras; violación de la privacidad o medidas de protección de los datos; fraude o falsificación informática; delitos informáticos relacionados con la identidad; delitos informáticos contra los derechos de propiedad intelectual y las marcas comerciales; actos informáticos que causen daños personales; actos informáticos que involucren racismo o xenofobia; producción, distribución o posesión informática de pornografía infantil; oferta o 'acicalado' (grooming) informáticos de niños; y actos informáticos en respaldo de delitos de terrorismo

Ello refleja un cierto consenso básico sobre las conductas culpables de delitos cibernéticos. Los países reportaron pocos delitos más que no se mencionan en el cuestionario. Estos se referían primordialmente al contenido informático, incluyendo la criminalización de material obsceno, el juego en línea y los mercados ilícitos en línea, como el de drogas y de personas.

Para esos 14 actos, los países reportaron el uso de delitos cibernéticos específicos correspondientes a actos básicos del delito cibernético contra la confidencialidad, la integridad y la accesibilidad de los sistemas informáticos.

Para otras formas de delito cibernético, se solían usar más a menudo figuras delictivas generales (no específicamente cibernéticas). Sin embargo, se comunicó que ambos enfoques se aplicaban para los actos informáticos que involucraban una violación de la privacidad, fraude o falsificación o un delito contra la identidad.

Aunque existe consenso a alto nivel sobre las áreas generales de criminalización, un análisis detallado de las disposiciones en la legislación fuente revela enfoques divergentes. Los delitos que involucran el acceso ilícito a sistemas informáticos y datos difieren con respecto al objeto del delito (datos, sistemas, o información), y con respecto a la criminalización solo del acceso o de requerir la intención, por ejemplo de ocasionar pérdidas o daños.

El requisito de la intención para la existencia de un delito también difiere en cuanto a los criterios de criminalización de la interferencia de datos o sistemas informáticos. La mayoría de los países exigen que la interferencia sea intencional, mientras que otros incluyen la interferencia temeraria.

En el caso de interferir datos informáticos, la conducta que constituye la interferencia va desde dañar hasta borrar, alterar, suprimir, agregar o transmitir datos. La criminalización de la intercepción ilegal difiere en virtud de si el delito se restringe a la transmisión de datos no públicos o no, y si el delito se restringe a la intercepción 'por medios técnicos'.

A modo de ejemplo, sólo parte de los países alcanzados tipifican como delito el uso indebido (o abusivo) de los dispositivos. En aquellos que lo hacen, surgen diferencias en cuanto a si el delito cubre la posesión, divulgación o el uso de programas informáticos (como también los programas maliciosos) y/o códigos de

acceso a computadoras (como las contraseñas de las víctimas). Desde la perspectiva de la cooperación internacional, dichas diferencias podrían tener impacto en las conclusiones de doble incriminación entre los países. Como veremos más adelante, justamente en este tipo penal es donde Argentina ha realizado sus reservas al momento de adherir al Convenio de Budapest.

Otro aspecto que destacamos, a modo de cierre de este estudio, es que varios de los países analizados han adoptado figuras delictivas cibernéticas específicas para el fraude, la falsificación y los delitos contra la identidad relacionados con la informática, donde hay gran consenso a nivel mundial. Otros extienden el ámbito de aplicación de las disposiciones generales sobre el fraude o el robo, o recurren a delitos que cubren elementos constitutivos – como el acceso ilícito, la interferencia o la falsificación de datos, en el caso de los delitos contra la identidad. Una variedad de delitos relacionados con el contenido, particularmente aquellos que involucran la pornografía infantil, muestran una amplia criminalización.

4.3. Instrumentos Internacionales sobre Ciberdelito

En las últimas dos décadas se han visto avances considerables en la promulgación de instrumentos internacionales y regionales dirigidos a contrarrestar el delito cibernético. Estos incluyen instrumentos vinculantes y no vinculantes.

Además de la membresía formal y de la aplicación de sus disposiciones, los instrumentos multilaterales sobre delito cibernético han influido indirectamente en las leyes nacionales, al ser usados como modelo por los Estados no miembro[171], o por influencia de la legislación de los Estados parte en otros países.

La membresía a un instrumento multilateral sobre delito cibernético se corresponde con la percepción de una mayor suficiencia de la legislación penal y procesal nacional, lo cual señala que las disposiciones multilaterales actuales en esas áreas se consideran, en general, efectivas.

[171] Consideración aplicable para la República Argentina, toda vez que al momento de la redacción en el año 2008 de la actual Ley Nº 26.388, si bien aún no había una adhesión formal, si se tuvo en cuenta el Convenio de Cibercrimen de Budapest.

4.3.1. Convenio sobre Ciberdelincuencia Nº 185: (Budapest)

Comenzaremos por el más reconocido a nivel internacional, al menos al momento de la redacción de la presente tesis: El Convenio sobre Ciberdelincuencia del Consejo de Europa (más conocido como el Convenio de Budapest[172]).

Esta Convención fue firmada en Budapest en 2001, entró en vigencia el 1ro. de Julio de 2004 y en su redacción participaron los 41 países miembros del Consejo de Europa, junto a otros Estados no miembros como Estados Unidos, Canadá, Japón y Sudáfrica.

El objetivo de este instrumento es recurrir a la colaboración internacional entre países, buscando desde el punto de vista penal de fondo, establecer un criterio de figuras penales mínimas o básicas que todos los Estados miembros asumen la obligación de tipificar. No obstante, en determinados tipos penales la Convención ofrece cierto grado de flexibilidad normativa, así como la posibilidad de realizar ciertas reservas.

Según el propio informe explicativo del Consejo de Europa sobre el Convenio[173], el mismo tiene como finalidad primordial:

> 1) armonizar los elementos de los delitos conforme al derecho sustantivo penal de cada país y las disposiciones conexas en materia de delitos informáticos;
>
> 2) establecer conforme al derecho procesal penal de cada país los poderes necesarios para la investigación y el procesamiento de dichos delitos, así como también de otros delitos cometidos mediante el uso de un sistema informático o las pruebas conexas que se encuentren en formato electrónico,
>
> 3) establecer un régimen rápido y eficaz de cooperación internacional.

---

[172] COUNCIL OF EUROPE. "Convenio de Cibercriminalidad de Budapest". Budapest, 23 de noviembre de 2001. Url: http://www.coe.int/t/dghl/standardsetting/t-cy/ETS_185_spanish.pdf , Consultado: 27 de Junio de 2017

[173] Consejo de Europa, STE núm. 185, Informe Explicativo - CONVENIO SOBRE LA CIBERDELINCUENCIA; Disponible en Url: https://rm.coe.int/16802fa403

Como afirma Walter Perron[174], el Convenio tiene un alcance que va más allá de los Estados miembros de la Unión Europea, cuyo núcleo está expuesto en la Convención Europea sobre derechos humanos. El Consejo no tiene facultades soberanas propias, sino que su objeto es influir en el desarrollo de los Estados miembros a través de recomendaciones y tratados. Su instrumento más importante es el Tribunal Europeo de Derechos Humanos (TEDH), cuya jurisprudencia es de superlativa importancia y ante el que todo ciudadano de un estado miembro puede comparecer en el marco de una petición individual.

De acuerdo a lo trabajado impecablemente por el Dr. Marcelo Riquert[175], el citado Convenio se ha constituido en una referencia insoslayable en términos de armonización legislativa en la materia y que la normativa argentina no tiene al presente mayor problema de compatibilidad con los estándares mínimos que aquél reclama en lo referente al derecho penal sustancial. Prueba de ello es la adhesión de Argentina sin mayores problemas, a través de la Ley Nro. 27.411, con determinadas reservas[176].

Volviendo al Convenio sobre Ciberdelincuencia del Consejo de Europa, el mismo fue el instrumento multilateral más usado para elaborar legislación sobre

---

[174] PERRON, Walter, "Perspectivas de la unificación del derecho penal y del derecho procesal en el marco de la Unión Europea", en AAVV, Estudios sobre Justicia Penal. Homenaje al Profesor Julio B. J. Maier, Bs. As., Editores del Puerto, 2005, pp. 734/735 y 737/738.

[175] Riquert, Marcelo, "Delincuencia informática y control social: ¿excusa y consecuencia?", en Revista Jurídica Facultad de Derecho de la UNMDP, n° 6, 2011, pp. 67/99; y [en línea] http://perso.unifr.ch/derechopenal/assets/files/articulos/a_20120208_01.pdf

[176] Las reservas han sido: a) La REPÚBLICA ARGENTINA hace reserva del artículo 6.1.b. del CONVENIO SOBRE CIBERDELITO y manifiesta que no regirá en su jurisdicción por entender que prevé un supuesto de anticipación de la pena mediante la tipificación de actos preparatorios, ajeno a su tradición legislativa en materia jurídico penal. b) La REPÚBLICA ARGENTINA hace reserva de los artículos 9.1.d., 9.2.b. y 9.2.c. del CONVENIO SOBRE CIBERDELITO y manifiesta que estos no regirán en su jurisdicción por entender que son supuestos que resultan incompatibles con el CÓDIGO PENAL vigente, conforme a la reforma introducida por la ley 26.388. c) La REPÚBLICA ARGENTINA hace reserva parcial del artículo 9.1.e. del CONVENIO SOBRE CIBERDELITO y manifiesta que no regirá en su jurisdicción por entender que el mismo sólo es aplicable de acuerdo a legislación penal vigente hasta la fecha, cuando la posesión allí referida fuera cometida con inequívocos fines de distribución o comercialización (artículo 128, segundo párrafo, del CÓDIGO PENAL). d) La REPÚBLICA ARGENTINA hace reserva del artículo 22.1.d. del CONVENIO SOBRE CIBERDELITO y manifiesta que no regirá en su jurisdicción por entender que su contenido difiere de las reglas que rigen la definición de la competencia penal nacional. e) La REPÚBLICA ARGENTINA hace reserva del artículo 29.4 del CONVENIO SOBRE CIBERDELITO y manifiesta que no regirá en su jurisdicción por entender que el requisito de la doble incriminación es una de las bases fundamentales de la LEY DE COOPERACIÓN INTERNACIONAL EN MATERIA PENAL N° 24.767 para el tipo de medidas de cooperación previstas en artículo y numeral citados.

delito cibernético. En conjunto, en la mitad de ese total de países se utilizaban instrumentos multilaterales de otros "grupos".

En general, un tercio de los países encuestados por el estudio de Naciones Unidas previamente citado reportaron que su legislación está altamente o muy altamente armonizada con la de los países considerados importantes con miras a la cooperación internacional. Sin embargo, esto varía a nivel regional, con mayores grados de armonización en las Américas y Europa. Ello puede deberse al uso, en algunas regiones, de instrumentos multilaterales que están diseñados inherentemente para que influyan en la armonización.

La fragmentación a nivel internacional, y la diversidad de leyes nacionales, en términos de los actos tipificados como delitos cibernéticos, las bases jurisdiccionales y los mecanismos para la cooperación, podrían estar correlacionadas con la existencia de múltiples instrumentos sobre el delito cibernético con distinto alcance temático y geográfico.

El Capítulo II del Convenio nos trae medidas que deberán adoptarse a nivel nacional (Artículos 2 a 22), donde contiene tres secciones: derecho penal sustantivo (artículos 2 a 13); derecho procesal (artículos 14 a 21) y jurisdicción (artículo 22).

Según se explica en el considerando Nº 33, la Sección 1 (Derecho penal sustantivo - art. 2 a 13), "*tiene como finalidad mejorar los medios para prevenir y evitar los delitos informáticos o los delitos relacionados con la informática al establecer una norma mínima común en relación con los delitos pertinentes. Este tipo de armonización facilita la lucha contra tales delitos en los ámbitos nacional e internacional. Si existen correspondencias entre las distintas leyes nacionales se pueden evitar abusos tales como el traslado del proceso a una Parte que aplique normas anteriores y sanciones menores. Por consiguiente, podría mejorar también el intercambio de experiencias comunes útiles en el manejo práctico de los casos. La cooperación internacional (especialmente la extradición y la asistencia judicial recíproca) se ve facilitada, por ej., respecto de los requisitos de doble tipificación penal.*"

Vale destacar que el desarrollo de dicho convenio en materia penal material se basa en gran medida en las directrices desarrolladas en relación con la Recomendación núm. R(89) del Consejo de Europa sobre delitos relacionados con

el empleo de ordenadores y en el trabajo de otras organizaciones internacionales de carácter público o privado (OCDE, Naciones Unidas, AIDP).

4.3.1.1. Primer Protocolo Adicional relativo a la penalización de actos de naturaleza racista y xenófoba cometidos a través de sistemas informáticos (STCE 189)

El Primer Protocolo Adicional al Convenio sobre Cibercrimen de Budapest representa un paso significativo en la cooperación internacional para abordar los desafíos emergentes relacionados con el cibercrimen.

Este protocolo adicional fue negociado entre finales de 2001 y comienzos del año 2002. El texto final de este protocolo fue nominado por el Consejo de Comité de Europa de Ministros el 7 de noviembre de 2002 bajo el título "Protocolo adicional al Convenio sobre la Ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos.

Como resultado de la constante labor de revisión de las disposiciones del Convenio por parte del T-CY, sobre la base de lo dispuesto en el artículo 46 del tratado, en enero de 2003, se publicó el primer protocolo adicional, que se refiere a la incriminación de los actos de carácter racista cometidos a través de sistemas informáticos[177], y que entró en vigor en 2006. El texto, elaborado en su mayor parte por un comité de redacción constituido en el contexto del T-CY —y posteriormente sometido a la evaluación de los Estados miembros— tiene como principal objetivo promover una mayor armonización entre legislaciones relevantes en el ámbito del derecho criminal sobre la lucha contra el racismo y la xenofobia en internet.

En cuanto a las cuestiones de procedimiento en torno a la actuación del TC-Y y su papel en la elaboración de protocolos adicionales al Convenio de Budapest, conviene aclarar que el colegiado puede debatir sugerencias de protocolos adicionales y elaborar borradores de los textos. Sin embargo, la decisión de adopción de un determinado protocolo o convenio adicional al tratado principal debe ser refrendada por el Comité de Ministros del Consejo de Europa y, tras su

[177] Consejo de Europa. Details of Treaty No.189. Disponible en: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=189

aprobación, el texto queda abierto a la adhesión de los Estados signatarios del convenio - por tanto, la adhesión a los protocolos adicionales al Convenio de Budapest no es realizada de forma automática por todos los Estados signatarios.

De acuerdo con el memorando explicativo[178] del texto, el acercamiento de partes distantes del mundo a través de los recientes cambios tecnológicos, comerciales y económicos, sería el motivo de una mayor incidencia y crecimiento acelerado de la difusión de contenidos de discriminación racial, xenofobia y otras formas de intolerancia en el ámbito online. En función de eso, el texto ofrece una definición para "material racista y xenófobo" (artículo 2) y tiene como objetivo presentar soluciones comunes para reprimir la difusión de este tipo de contenidos a través de los sistemas informáticos.

A continuación, aportamos un resumen del contenido aportado por este Primer Protocolo Adicional al Convenio de Budapest.

Temas	Artículos
Disposiciones Comunes y cuestiones generales	Capítulo I - Disposiciones Comunes
Disposiciones comunes y cuestiones generales	Capítulo II • Medidas a ser tomadas a nivel nacional • Difusión de contenidos racistas y xenófobos por sistemas • Amenazas por motivos racistas y xenófobos • Insultos por motivos racistas y xenófobos • Negación, minimización, aprobación o justificación de genocidios y crímenes contra la humanidad
Relación entre el Convenio de Budapest y el Protocolo Adicional	Capítulo III - Relaciones entre el Convenio y el Protocolo
Disposiciones Finales	Capítulo IV – Disposiciones finales

Destacamos como un aspecto importante sobre el primer protocolo adicional es el intento de establecer una dinámica equilibrada entre la libertad de expresión de

[178] Consejo de Europa. Explanatory Report to the Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems. 2003. Disponible en: https://rm.coe.int/1680989b1c

los usuarios de Internet y una lucha eficaz contra la difusión y la práctica del racismo y la xenofobia en el ámbito digital.

En el Artículo 6, Sección 1 del Protocolo se refiere específicamente a la negación del Holocausto y otros genocidios reconocidos como tales por otros tribunales internacionales establecidos desde 1945 por los instrumentos jurídicos internacionales pertinentes. La sección 2 del artículo 6 permite a las Partes en el Protocolo perseguir delitos a su sola discreción si el delito se comete con la intención de incitar al odio, la discriminación o la violencia; o para hacer uso de una reserva, al permitir que una Parte no aplique - en su totalidad o en parte - el artículo 6.

De nuestra investigación podemos concluir que casi no hemos encontrado críticas o cuestionamientos hacia este primer protocolo. En parte puede ser por su cercanía con el convenio en sí mismo, y que muchos países al momento de la adhesión al Convenio, ya incluían la adhesión a este primer protocolo adicional.

Por otro lado, puede deberse a la materia abordada, sobre la cual existe un amplio consenso en relación a mejorar herramientas que permitan combatir un flagelo tan complicado como los discursos racistas y de odio, donde las nuevas tecnologías tienen un rol fundamental.

A modo de detalle de algunas controversias que ha generado este primer protocolo, lo único que podemos mencionar que el gobierno de Estados Unidos no cree que la versión final del Protocolo sea compatible con las garantías constitucionales de los Estados Unidos e informó al Consejo de Europa que no adherirá a este protocolo.

Al momento de la redacción de estas líneas, según el sitio oficial del Consejo[179] de Europa, el número total de firmas no seguidas de ratificaciones eran 10 y el número total de ratificaciones/adhesiones eran 35.

[179] COUNCIL OF EUROPE: “Chart of signatures and ratifications of Treaty 189”; Disponible en: Url: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=189

4.3.1.2. Segundo Protocolo adicional al Convenio sobre la Ciberdelincuencia, relativo a la cooperación reforzada y la revelación de pruebas electrónicas.

Este segundo protocolo adicional[180] busca garantizar la coordinación y cooperación internacional en las investigaciones y procedimientos criminales contra el ciberdelito, así como también mejorar la capacidad de las autoridades de la justicia penal para recoger evidencia digital en el marco de estos procedimientos.

El texto surgió una vez más de una decisión del T-CY sobre la necesidad de endurecer las normas –como se destaca en su memorando explicativo–[181], especialmente en lo que dice respecto a la divulgación de informaciones de registro de nombres de dominio, medidas de cooperación directa con proveedores de servicios para la obtención de informaciones de usuarios, medios eficaces para la obtención de informaciones de usuarios y datos de tráfico, cooperación inmediata en casos de emergencia, herramientas de asistencia mutua, así como salvaguardias para la preservación de los derechos humanos en el ámbito digital.

El contexto para la creación del segundo protocolo adicional es, sin embargo, relativamente más complejo que el primero[182]. Con el fin de aportar complementos al texto del Convenio de Budapest, el TC-Y creó dos grupos Ad Hoc dedicados exclusivamente al acceso fronterizo a los datos y cuestiones de jurisdicción territorial (Transborder Group[183], creado en 2012) y el acceso a los datos almacenados en las nubes (Cloud Evidence Group, creado en 2015[184]). En el año 2016, el final de los debates del Cloud Evidence Group llegó a la conclusión de que existía una supuesta dificultad de los Estados para acceder a los datos privados en función de cuestiones como la territorialidad, la computación en la nube y el alcance de las

[180] COUNCIL OF EUROPE: Disponible en: https://www.coe.int/en/web/cybercrime/second-additional-protocol

[181] Consejo de Europa. Explanatory Report to the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence. 2022. Disponible en: https://rm.coe.int/1680a49c9d

[182] Derechos Digitales América Latina; "Convenio de Budapest sobre la Ciberdelincuencia en América Latina: Un breve análisis sobre adhesión e implementación en Argentina, Brasil, Chile, Colombia y México", Disponible en: https://www.derechosdigitales.org/wp-content/uploads/ESP-Ciberdelincuencia-2022.pdf

[183] Consejo de Europa. Transborder Ad Hoc Group. Disponible en: https://www.coe.int/en/web/cybercrime/tb

[184] Consejo de Europa. Cloud Evidence Ad Hoc Group. Disponible en: https://www.coe.int/en/web/cybercrime/ceg

jurisdicciones[185]. Debido a las limitaciones discutidas en el colegiado, la conclusión terminó siendo la elaboración de un nuevo protocolo adicional que fue discutido entre 2017 y 2021.

De acuerdo con el Consejo de Europa[186], el segundo protocolo surge como una actualización necesaria para convertir el Convenio de Budapest en un instrumento más eficaz al tiempo que revisa cuestiones como el acceso transfronterizo a los datos y la cooperación legal mutua, y establece parámetros más claros para la cooperación directa entre las autoridades y los proveedores de servicios digitales, inclusive en el nivel de los proveedores de servicios de infraestructura de internet.

Respecto a los procedimientos para mejorar la cooperación directa con proveedores y entidades de otras partes, el Protocolo establece que las partes podrán solicitar información a entidades prestadores de servicios de registro de nombres de dominio para identificar o contactar a un titular de dominio. Asimismo, contempla la posibilidad de que las partes soliciten información específica sobre sus abonados a los prestadores de servicios dentro de su territorio.

En una primera mirada el Protocolo se encuentra estructurado de la siguiente forma:

Temas	Artículos
Disposiciones Generales	Capítulo I - Disposiciones Comunes
Cooperación Mejorada	Capítulo II - Medidas para el mejoramiento de la cooperación — Sección I - Principios Generales — Sección II - Procedimientos para el mejoramiento de la cooperación con proveedores de servicios y otras partes — Sección III - Procedimientos para el mejoramiento de la cooperación internacional entre autoridades para el intercambio de datos — Sección IV - procedimientos para Asistencia Mutua

[185] inCyber. [Budapest Convention] A second protocol to fight cybercrime. Diciembre, 2021. Disponible en: https://incyber.fr/en/budapest-convention-a-second-protocol-to-fight-cybercrime/

[186] CCDCOE. Battling Cybercrime Through the New Additional Protocol to the Budapest Convention. 2021. Disponible en: https://ccdcoe.org/library/publications/battling-cybercrime-through-the-new-additional-protocol-to-the-budapest-convention/

	— Sección V - Procedimientos relativos a actividades de cooperación internacional en ausencia de acuerdos internacionales
Condiciones, Salvaguardas y derechos	Capítulo III - Condiciones y Salvaguardas — Protección de datos personales — Salvaguardas — Principios Generales
Disposiciones Finales y asuntos de procedimiento	Capítulo IV - Efectos del Protocolo, firma, reservas, etc.

- procedimientos para mejorar la cooperación directa con proveedores y entidades de otras partes;
- procedimientos para mejorar la cooperación internacional entre autoridades para la divulgar datos informáticos almacenados;
- procedimientos concernientes a la asistencia mutua en caso de emergencia; y
- procedimientos concernientes a la cooperación internacional en ausencia de acuerdos internacionales aplicables.

Un aspecto relevante es que las partes podrán solicitar a las autoridades ser notificadas simultáneamente. Por su parte, las autoridades tendrán la facultad de impedir la divulgación de la información si ésta pudiese perjudicar investigaciones o procedimientos penales, o si los supuestos contemplados para denegar la asistencia mutua establecidos en el Convenio se cumplieran.

A su vez, el Protocolo contempla procedimientos para mejorar la cooperación internacional entre autoridades para divulgar datos informáticos almacenados. Esto significa que introduce medidas para que las partes colaboren gobierno a gobierno, facultando a sus autoridades competentes a obligar a proveedores de servicios a brindar información sobre los abonados y sobre datos de tráfico. Además, establece que las partes puedan adoptar las medidas necesarias en situación de emergencia para que su punto de contacto solicite al punto de contacto de otra parte asistencia inmediata para acelerar la divulgación de los datos específicos informáticos por parte de un proveedor de servicios sin mediar previamente una solicitud de asistencia.

El Protocolo también incluye procedimientos concernientes a la asistencia mutua en caso de emergencia. En ese sentido, las partes podrán solicitar asistencia

mutua de forma rápida y expedita cuando alguno considere que existe una emergencia. Para ello, las partes deberán detallar hechos suficientes que justifiquen la emergencia y la relación de los datos solicitados con ella. Las partes requeridas decidirán sobre la solicitud de forma expeditiva y en qué condiciones se proveerá la información.

En cuanto a los procedimientos relativos a la cooperación internacional en ausencia de acuerdos internacionales aplicables, el Protocolo introduce herramientas como la videoconferencia para tomar testimonios y declaraciones de un testigo o perito, con el acuerdo previo de las partes sobre aspectos procesales en los que se garanticen derechos de los intervinientes, se regule la intervención de los peritos y testigos y se acuerden formalidades propias de los procedimientos judiciales. Asimismo, las partes pueden crear y poner en funcionamiento equipos conjuntos de investigaciones para facilitar las investigaciones o los procedimientos penales.

Sobre el final de este trabajo, ahondaremos en un repaso de las medidas de investigación propiamente dichas que aporta este instrumento, a fin de ser tenidas en cuenta en la propuesta final de esta tesis.

Las disposiciones finales del Protocolo permiten a las partes aplicar acuerdos internacionales bilaterales de protección de datos personales. Además, las disposiciones establecen que la parte que haya recibido los datos de carácter personal deberá tratarlos según los fines establecidos en el Protocolo, para garantizar su exactitud, integridad y actualización, y regular el tratamiento de datos sensibles, el período de conservación y las decisiones automatizadas. El Protocolo plantea que las partes deberán informar al titular sobre el tratamiento, la conservación y la accesibilidad, rectificación y revisión de los datos personales.

Por último, el Protocolo establece que las partes deberán garantizar medidas tecnológicas, físicas y organizativas adecuadas para proteger los datos personales de su pérdida, acceso, difusión alteración o su destrucción accidental o no autorizada. El Protocolo regula la actuación de las partes ante la detección de un incidente de seguridad que dañe a las personas o a la otra parte, como así también su notificación cuando afecte la seguridad nacional o seguridad pública. Asimismo, entre otros aspectos, establece la suspensión de la transferencia de datos

personales por motivos de incumplimiento al Protocolo o riesgo significativo e inminente para la vida o la seguridad de una persona física, o un perjuicio sustancial para su reputación o su patrimonio.

Argentina firmó el Segundo Protocolo Adicional el 16 de febrero de 2023. Al momento de la redacción de esta líneas, Argentina aún deberá cumplir con el correspondiente trámite legislativo previsto constitucionalmente para resolver respecto de su aprobación y/o determinación de reservas.

4.3.1.3. Críticas y cuestionamientos al Segundo Protocolo adicional al Convenio sobre la Ciberdelincuencia.

A diferencia de lo ocurrido con el primer protocolo adicional, este segundo protocolo ha suscitado una variada gama de críticas y cuestionamientos por parte de importantes organizaciones internacionales dedicadas a la protección de los derechos y garantías de la sociedad civil.

Expertos de la Electronic Frontier Foundation (EFF), probablemente la organización dedicada a la protección de la privacidad más importante a nivel mundial, afirman que en el proceso de la redacción de este segundo protocolo por parte del Comité de Ciberdelincuencia del CdE (T-CY) estuvo fuertemente influenciado por los agentes de seguridad pública y de las fuerzas del orden[187] .

Los grupos de derechos humanos y digitales, los abogados defensores e incluso los reguladores de la protección de datos fueron en gran medida marginados durante el proceso de redacción, lo que fue señalado por las organizaciones de la sociedad civil[188]. Afirman entonces que el texto resultante es una expresión de este proceso desigual, con salvaguardias obligatorias de derechos humanos que no son

[187] Katitza Rodríguez, Tamir Israel. Global Law Enforcement Convention Weakens Privacy & Human Rights, 8 de junio de 2021. Url: https://www.eff.org/deeplinks/2021/06/global-law-enforcement-convention-weakens-privacy-human-rights

[188] El Consejo Europeo de Protección de Datos (CEPD), en las presentaciones del organismo a las consultas del TC-Y para el proyecto de texto del Protocolo, ha subrayado repetidamente la importancia de involucrar a las autoridades de protección de datos en el proceso de redacción del Protocolo. Véase la contribución del CEPD en noviembre de 2019. Url: https://www.eff.org/deeplinks/2021/07/council-europes-actions-belie-its-pledges-involve-civil-society-development-cross y la declaración del CEPD en febrero de 2021; Url: https://edpb.europa.eu/our-work-tools/our-documents/statements/statement-022021-new-draft-provisions-second-additional_en

tan sólidas como las obligaciones que facilitan el acceso policial transfronterizo a los datos personales.

Considerando que la importancia de estos aspectos es radical para este trabajo y entendiendo que la construcción de este marco teórico apunta precisamente a poder tener la estructura necesaria para realizar dichas consideraciones y cuestionamientos sobre la afectación de los derechos y garantías a partir de las medidas de investigación, prometemos al lector que la profundización sobre las mismas serán adecuada y debidamente abordadas en los últimos capítulo de esta tesis.

4.3.1.4. Aspectos destacados del Convenio

Algunos de los aspectos más destacados del texto en las actividades conmemorativas de su vigésimo primer aniversario en 2021 fueron el potencial para fomentar las estructuras de cooperación público-privada y la armonización entre las legislaciones y otras [189]estructuras legales y administrativas dedicadas a la lucha contra los ciberdelitos.

En este sentido, es importante señalar que a pesar del tenor punitivo bajo el cual fue elaborado el Convenio de Budapest, su relevancia hoy en día se debe al constante trabajo de actualización y a partir de cierto nivel de interlocución con otras discusiones como las relacionadas con la defensa de los derechos humanos en la era digital.

En los últimos años, el tratado se ha consolidado de hecho como una base legal inicial para la definición de las estructuras de cooperación internacional, así como una guía para la posterior elaboración de legislaciones nacionales.

El Convenio también cuenta con un Comité específico - Cybercrime Convention Committee (T-CY)[190] - que es responsable de debatir las mejoras y actualizaciones del texto, y está compuesto por todos los países que han firmado o han sido invitados a firmar el Tratado.

[189] CONSEJO DE EUROPA: Benefits. Disonible en: https://www.coe.int/en/web/cybercrime/benefits
[190] Cybercrime Convention Committee (T-CY). The Budapest Convention on Cybercrime: benefits and impact in practice. Disponible en: https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac

La creación del Comité T-CY está motivada por el artículo 46[191] del Convenio, que refuerza la necesidad de un mecanismo de consulta periódica entre los firmantes, con el objetivo principal de promover el intercambio de información sobre el uso y la implementación del texto, los procesos recientes de innovaciones tecnológicas y legislativas sobre la lucha contra los ciberdelitos y la recopilación de pruebas digitales, y también la discusión de posibles suplementos o adiciones al texto del convenio.

Asimismo, el colegiado ha funcionado como uno de los grupos intergubernamentales más relevantes actualmente para el debate y el análisis de la implementación del Convenio, así como para la elaboración de interpretaciones del texto mediante notas orientativas (guidance notes[192]). Desde la creación del convenio, se han elaborado notas orientativas sobre temas como los sistemas informáticos, botnets, ataques DDoS, spam, terrorismo, entre otros.

Aún en relación al TC-Y, vale la pena mencionar que el Comité es el principal espacio de intercambio de información sobre la implementación y uso del Convenio y tiene el mandato para elaborar protocolos adicionales al texto original para articular nuevas cuestiones y demandas de los estados miembros en la lucha contra la ciberdelincuencia. De acuerdo con el reglamento interno del órgano (Rules of Procedure[193]), el mandato permite al colegiado realizar evaluaciones sobre la

[191] *Article 46 – Consultations of the Parties*

1. The Parties shall, as appropriate, consult periodically with a view to facilitating:

A. the effective use and implementation of this Convention, including the identification of any problems thereof, as well as the effects of any declaration or reservation made under this Convention;

B. the exchange of information on significant legal, policy or technological developments pertaining to cybercrime and the collection of evidence in electronic form;

C. consideration of possible supplementation or amendment of the Convention.

2. The European Committee on Crime Problems (CDPC) shall be kept periodically informed regarding the result of consultations referred to in paragraph 1.

3. The CDPC shall, as appropriate, facilitate the consultations referred to in paragraph 1 and take the measures necessary to assist the Parties in their efforts to supplement or amend the Convention. At the latest three years after the present Convention enters into force, the European Committee on Crime Problems (CDPC) shall, in co-operation

with the Parties, conduct a review of all of the Convention's provisions and, if necessary, recommend any appropriate amendments.

4. Except where assumed by the Council of Europe, expenses incurred in carrying out the provisions of paragraph 1 shall be borne by the Parties in the manner to be determined by them.

5. The Parties shall be assisted by the Secretariat of the Council of Europe in carrying out their functions pursuant to this article.

[192] Consejo de Europa. Guidance Notes on the Convention on Cybercrime. Disponible en: https://www.coe.int/en/web/cybercrime/guidance-notes

[193] Consejo de Europa. Cybercrime Convention Committee (T-CY) T-CY Rules of Procedure. Octubre, 2020. Disponíble en: https://rm.coe.int/t-cy-rules-of-procedure/1680a00f34

aplicación y el impacto del Convenio, adoptar opiniones y recomendaciones sobre posibles interpretaciones respecto del texto y debatir la elaboración de instrumentos legales —como convenios y protocolos adicionales— sobre cuestiones relacionadas con el Convenio de Budapest para someterlos a la aprobación del Comité de Ministros del Consejo de Europa.

Otro punto relevante en cuanto a la estructura del Convenio es la red 24/7, establecida por el artículo 35[194], que consiste en una red de puntos de contacto en todos los países firmantes y cuyos representantes tienen que estar disponibles para prestar asistencia inmediata tan pronto como les sea requerida. El objetivo principal de la citada red es establecer un canal de asistencia a efectos de investigaciones, procedimientos relativos a crímenes cibernéticos o incluso la recolección de pruebas electrónicas.

De acuerdo a lo que regule cada Estado, la red 24/7 también puede ser la responsable de proporcionar conocimientos técnicos, aplicar medidas de preservación/protección de datos y recopilar pruebas digitales, incluso información sobre la ubicación de los sospechosos.

Por último, cabe mencionar que el acceso/adhesión al Convenio también ofrece a los firmantes la posibilidad de llevar a cabo actividades de concientización y capacitación por parte del Comité Europeo. En un mundo en el que la disputa sobre el régimen de acceso a los datos localizados en el extranjero es un tema recurrente, abordado en muchas legislaciones y proyectos de ley en discusión, es relevante que la estructura facilitada por el Convenio pueda promover actividades de capacitación

---

[194] *Article 35 – 24/7 Network*

Each Party shall designate a point of contact available on a twenty-four hour, seven-day-aweek basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures

1. A. the provision of technical advice;

B. the preservation of data pursuant to Articles 29 and 30;

C. the collection of evidence, the provision of legal information, and locating of suspects.

2. A. A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis.

B. If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis.

3. Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.

para los actores, incluso si esta medida es accesible, en gran medida, solo para los representantes de los Estados signatarios. Muchas de sus actividades de capacitación son difundidas en el sitio propio del Consejo de Europa, en la sección dedicada al Convenio[195].

4.3.1.5. Argentina y el Convenio sobre la Ciberdelincuencia de Budapest

Ya en el año 2008, cuando Argentina sancionó la Ley de Delitos Informáticos N° 26.338, e incorporó una serie de delitos al Código Penal, se había tomando como modelo las normas del Convenio, por lo que se contaba, al menos en el campo del derecho penal material, de los elementos mínimos como para avanzar hacia una adhesión.

Sin embargo, su adhesión se demoró varios años y recién en 2018, con motivo de la sanción de la Ley Nº 27.41135, el país internalizó las disposiciones del Convenio de Budapest en su ordenamiento jurídico.

La adhesión de Argentina, sin embargo, se hizo con reservas debido a las disposiciones que representaban un conflicto potencial con la legislación nacional. Deja fuera, por tanto, las disposiciones relacionadas mayormente a las medidas relativas a la pornografía infantil y a las cuestiones jurisdiccionales.

A continuación generamos un cuadro donde pueden visualizar las reservas realizadas por la República Argentina:

Argentina: Artículos de Reserva	Textos del Convenio de Cibercrimen de Budapest
Art. 6.1.b	**Artículo 6 - Abuso de los dispositivos** 1. Cada Parte adoptará las medidas legislativas y de otro tipo que sean necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de los siguientes actos (...) B. la posesión de alguno de los elementos contemplados en los anteriores incisos i) o ii) del apartado a) con el fin de que sean utilizados para cometer cualquiera de los delitos previstos en los artículos 2 a 5. Cualquier Parte podrá exigir en su derecho interno que se posea un número determinado de dichos elementos para que se considere que existe responsabilidad penal.

[195] Disponible en: https://www.coe.int/en/web/cybercrime/capacity-building-programmes

Art. 9.1.d	**Artículo 9 - Delitos relacionados con la pornografía infantil** 1. Cada Parte adoptará las medidas legislativas y de otro tipo que sean necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de los siguientes actos: (...) D. la adquisición de pornografía infantil por medio de un sistema informático para uno mismo o para terceros;
Art. 9.1.e	**Artículo 9 - Delitos relacionados con la pornografía infantil** 1. Cada Parte adoptará las medidas legislativas y de otro tipo que sean necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de los siguientes actos: (...) E. la posesión de pornografía infantil en un sistema informático o en un dispositivo de almacenamiento de datos informáticos.
Art. 9.2.b	**Artículo 9 - Delitos relacionados con la pornografía infantil** 2.A los efectos del anterior párrafo 1, por "pornografía infantil" se entenderá todo material pornográfico que contenga la representación visual de:: (...) B. una persona que parezca un menor comportándose de una forma sexualmente explícita
Art. 9.2.c	**Artículo 9 - Delitos relacionados con la pornografía infantil** 2.A los efectos del anterior párrafo 1, por "pornografía infantil" se entenderá todo material pornográfico que contenga la representación visual de:: (...) C. imágenes realistas que representen a un menor comportándose de una forma sexualmente explícita.
Art. 22.1.d.	**Artículo 22 - Jurisdicción** 1. Cada Parte adoptará las medidas legislativas y de otro tipo que sean necesarias para afirmar su jurisdicción respecto de cualquier delito previsto con arreglo a los artículos 2 a 11 del presente Convenio, siempre que se haya cometido:(..) D. por uno de sus nacionales, si el delito es susceptible de sanción penal en el lugar en el que se cometió o si ningún Estado tiene competencia territorial respecto del mismo.
Art. 29.4.	**Artículo 29 - Conservación rápida de datos informáticos almacenados** 4. Cuando una Parte exija la doble tipificación penal como condición para atender una solicitud de asistencia mutua para el registro o el acceso de forma similar, la confiscación o la obtención de forma similar o la revelación de datos almacenados, dicha Parte podrá reservarse, en relación con delitos distintos de los previstos con arreglo a los artículos 2 a ll del presente Convenio, el derecho a denegar la solicitud de conservación en virtud del presente artículo en los casos en que tenga motivos para creer que la condición de la doble tipificación penal no podrá cumplirse en el momento de la revelación.

El país ha informado de su participación activa en el Comité T-CY y ha celebrado la adopción del 2º Protocolo Adicional al Convenio de Budapest afirmando que "Para prevenir y perseguir el delito cibernético es fundamental contar con

mecanismos e instrumentos adecuados que permitan y faciliten la cooperación y asistencia internacional"[196].

Más adelante en este mismo trabajo, realizaremos un estudio de derecho comparado donde podremos advertir con mejor detalle el nivel de adecuación, tanto a nivel material como procesal de cada uno de los países alcanzados por el estudio.

4.3.1.6. Brasil y el Convenio sobre la Ciberdelincuencia de Budapest

A pesar de ser, desde hace más de 20 años, una demanda de sectores como Ministerios, agencias gubernamentales, el Ministerio Público federal y una parte del Congreso Nacional, la adhesión de Brasil al Convenio de Budapest sobre la Ciberdelincuencia sólo se aprobó[197] en diciembre de 2021 y espera el inicio del proceso de implementación.

Las discusiones en torno al tema han estado bastante presentes en el escenario legislativo brasileño y anteceden a la aprobación de leyes clave sobre el ámbito digital promulgadas en el país como el Marco Civil de Internet[198] y la Ley General de Protección de Datos Personales[199] así como algunas leyes ordinarias[200] que implicaron cambios en el Código Penal brasileño para incluir tipificaciones sobre delitos cibernéticos.

En los años 2000, un proyecto de ley sustitutivo de otros proyectos de ley relacionados con los delitos informáticos presentado por el senador Eduardo

---

[196] Ministerio de Seguridad. Ciberdelito: Se aprobó el texto del 2° Protocolo Adicional del Convenio de Budapest. Argentina. Mayo, 2021. Disponible en: https://www.argentina.gob.ar/noticias/ciberdelito-se-aprobo-el-texto-del-2deg-protocolo-adicional-del-convenio-de-budapest

[197] Gobierno Federal, Ministerio de Justicia y Seguridad Pública. Aprobada la adhesión de Brasil al Convenio de Budapest sobre la Ciberdelincuencia. Diciembre de 2021. Disponible en: https://www.gov.br/mj/pt-br/assuntos/noticias/aprovada-adesao-do-brasil-a-convencao-de-budapeste-sobre-o-crime-cibernetico

[198] Presidencia de la República de Brasil. Ley nº 12.965, de 23 de abril de 2014, que establece princípios, garantías, derechos y deberes para el uso de Internet en Brasil. Abril, 2014. Disponible en: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm

[199] Presidencia de la República de Brasil. Ley nº 13.709, de 14 de agosto de 2018, Ley General de Protección de Datos Personales (LGPD). Agosto, 2018. Disponible en: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

[200] Ejemplos relevantes de las actualizaciones realizadas en los últimos años en la legislación penal brasileña para abordar la lucha contra la ciberdelincuencia son la ley 12.737, de 30 de novembro de 2012, y Lei n. 14.155, de 27 de maio de 2021.

Azeredo (PL de la Cámara nº 89 de 2003[201]) ya intentaba promover algún nivel de armonización entre las tipificaciones y discusiones presentes en el Convenio de Budapest contra la Ciberdelincuencia. Este texto fue fuertemente combatido por entidades de la sociedad civil, activistas y académicos debido a las tipificaciones genéricas y ambivalentes que pretendía introducir en el sistema jurídico brasileño. En respuesta, se propuso una ley destinada a la protección y garantía de los derechos en el ámbito digital que desembocaría, en 2011, en el envío de una de las primeras versiones del texto del Marco Civil de Internet[202].

Aún en el Marco Civil de Internet (MCI), cabe destacar que el texto continuó prosperando como la principal legislación de internet en el país, especialmente por su abordaje basado en los derechos de los usuarios de internet y también porque su elaboración contó con la participación de los más diversos sectores de la sociedad brasileña. Sobre el tema específico de las investigaciones online y el almacenamiento de datos, el MCI contiene disposiciones sobre el almacenamiento y la disponibilidad de los registros de conexión y acceso a las aplicaciones de Internet. En 2018, siguiendo el ejemplo de elaboración normativa con la participación de la sociedad, el país aprobó la ley n. 13.709/2018, o Ley General de Protección de Datos Personales[203], responsable de establecer las reglas básicas para la ejecución de las actividades de tratamiento de datos personales en el país.

En el ámbito judicial, una sentencia del Supremo Tribunal Federal (STF) sellará una controversia sobre el Acuerdo de Asistencia Judicial en Materia Penal (MLAT), firmado entre Brasil y Estados Unidos. La duda que debe decidir el STF es si las autoridades brasileñas, incluido el poder judicial, pueden solicitar directamente a las empresas de tecnología en el extranjero datos e informaciones, prescindiendo así de los procedimientos de cooperación jurídica internacional para la obtención de contenidos de aplicaciones de internet que se encuentren en el extranjero. En 2020,

[201] Safernet Brasil. PL sobre Crimes Cibernéticos: Projeto de Lei Substitutivo do Senador Eduardo Azeredo (PSDB-MG). Disponible en: https://www.safernet.org.br/site/institucional/projetos/obsleg/pl-azeredo

[202] Cámara de Diputados. Projeto de ley n. 2126/2011, que establece principios, garantías, derechos y deberes para el uso de Internet en Brasil. Disponible en: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=517255

[203] Presidencia de la República de Brasil. Ley General de Protección de Datos Personales. Disponible en: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

el STF celebró una audiencia pública para escuchar a expertos en la materia[204], en la que se hizo referencia en varios momentos a los conceptos aportados por el Convenio de Budapest, así como a la necesidad de respetar los derechos humanos. En Febrero de 2023, el Tribunal, por mayoría, conoció del recurso de declaración de constitucionalidad. En cuanto al fondo, por unanimidad, aceptó parcialmente la solicitud formulada inicialmente para declarar la constitucionalidad de los señalados dispositivos y la posibilidad de solicitud directa de datos y comunicaciones electrónicas de las autoridades nacionales a las empresas tecnológicas, en las hipótesis específicas del art. 11 del Marco Civil de Internet y art. 18 del Convenio de Budapest, es decir, en los casos de actividades de recolección y procesamiento de datos en el país, posesión o control de datos por una empresa con representación en Brasil y delitos cometidos por personas físicas ubicadas en el territorio nacional, con comunicación de esta decisión a la Poder Legislativo y Poder Ejecutivo, para que adopten las medidas necesarias para mejorar el marco legislativo, con la discusión y aprobación del proyecto de Ley General de Protección de Datos para Fines Penales[205].

4.3.1.7. Colombia y el Convenio sobre la Ciberdelincuencia de Budapest

El 24 de julio de 2018 la República de Colombia, por medio de su Congreso, aprueba la Ley 1928 (2018)[206], con la cual aprueba el Convenio sobre la Ciberdelincuencia, sin embargo, uno de los requerimientos para poder adherirse a dicho convenio es presentar el instrumento de adhesión ante el Consejo de Europa en Estrasburgo, ante ello, de acuerdo con el mismo Consejo de Europa (2019):

El 3 de enero de 2018, María Ángela Holguín Cuellar, Ministra de Relaciones Exteriores de Colombia, solicitó una prórroga del plazo de adhesión de Colombia al Convenio sobre la Ciberdelincuencia (RCDE Nº 185), hasta el 12 de septiembre de 2020, a fin de disponer del tiempo necesario para completar el proceso interno de adhesión. (párr. 2)

---

[204] STF. Audiencia pública n. 29. Disponible en: http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADC51Transcricoes.pdf

[205] Superior Tribunal Federal de Brasil. Disponible en: https://portal.stf.jus.br/processos/detalhe.asp?incidente=5320379

[206] Disponible en: https://vlex.com.co/vid/ley-1928-24-julio-737603069

De esta manera, Colombia presentó su instrumento de adhesión en fecha 16 de marzo de 2020, entrando en vigor el 01 de julio de 2020.

En cuanto a las reservas en la instauración del tratado, la legislación colombiana no integró el artículo 20 y 21, los que se refieren a la intercepción y recolección de datos.

Es importante destacar que aún Colombia no estaba adherido al Consejo de Europa, por medio de la Ley 1273 publicada en año de 2009 se adoptaron los términos del Convenio sobre la Ciberdelincuencia en la legislación nacional, y de acuerdo con el Consejo de Europa (2021), en la contestación de la solicitud para adherirse al Convenio.

Es decir, de forma similar al caso de Argentina, el instrumento internacional, aún sin adhesión, fue tomado de referencia normativa al momento de legislar en materia de delitos informáticos.

En mayo de 2022 el gobierno colombiano emitió el Decreto 338[207], relacionado a seguridad digital. En el decreto, se busca fortalecer la gobernanza y penalización de delitos cibernéticos, materializando los esfuerzos estatales contra la ciberdelincuencia en proyectos como la disponibilidad de sistemas y servicios informáticos. Lo anterior pretende acercar a los usuarios al entorno digital.

En dicho documento se menciona la existencia de un Grupo de Respuesta a Emergencias Cibernéticas de Colombia – ColCERT, que asesora, apoya y coordina a las múltiples partes interesadas para la adecuada gestión de los riesgos e incidentes digitales. Así mismo, es el punto único de contacto y respuesta nacional que coopera y ayuda a responder de forma rápida y eficiente a los incidentes de seguridad digital. Por otro lado, se hace referencia al Equipo de Respuesta a Incidentes de Seguridad Cibernética - CSIRT GOBIERNO, definiendo que se trata de un equipo de Respuesta a Incidentes de Seguridad Digital para las autoridades de la administración pública con el objetivo de prevenir y gestionar los incidentes de Seguridad digital, en el marco del Modelo de Seguridad y Privacidad de la Política de Gobierno Digital.

[207] Gobierno de Colombia; Ministerio de Tecnologías de la Información y las Comunicaciones. Disponible en: https://gobiernodigital.mintic.gov.co/692/articles-238198_recurso_1.pdf

4.3.1.8. México y el Convenio sobre la Ciberdelincuencia de Budapest[208]

México históricamente ha firmado diversos tratados internacionales en diferentes materias, en específico, en la temática de los derechos humanos. En cada tratado ha tenido la obligación de reformar o crear legislaciones correspondientes, para todo lo anterior tenemos como ejemplo la reforma en materia de derechos humanos publicada en el Diario Oficial de la Federación con fecha 10 de junio de 2011[209] la cual modificó la manera de protección de los derechos humanos de todas las personas del territorio nacional, teniendo como consecuencia, la reforma constitucional respecto a los artículos 1, 3, 11, 15, 18, 29, 33, 89, 97, 102 apartado B y 105; sin embargo, en materia de delitos cibernéticos se ha abstenido de formar parte del Convenio de Budapest, teniendo, como ya se mencionó supra, un estatus de observador, de acuerdo con el Punto de Acuerdo presentado por la senadora Silvana Beltrones Sánchez, por el que exhorta a las autoridades del Ejecutivo Federal para que se concluya la evaluación al marco jurídico vigente que permitiría cumplir cabalmente con las obligaciones contenidas en el Convenio sobre la Ciberdelincuencia (Convenio de Budapest) para la adhesión al mismo, ante la comisión de relaciones exteriores.

En el año 2006, el entonces Observador Permanente Adjunto de México hizo la solicitud formal para la adhesión de nuestro país al Convenio sobre la Ciberdelincuencia. El 31 de enero de 2007, el Comité de Ministros del Consejo de Europa, hizo la invitación conducente. No obstante, la adhesión de México al Convenio de Budapest aún no ha sido ratificada por el Ejecutivo Federal.

Pese a que México fue invitado a ser parte del mencionado convenio, tomó la decisión de mantenerse al margen de este, teniendo como consecuencia que el Código Penal Federal solo contemple figuras jurídicas como son: sabotaje,

---

[208] ELIZALDE CASTAÑEDA, Rodolfo Rafae; FLORES RAMIREZ, Héctor Hugo; CASTRO LORZO, Edwin Misael: "Los delitos cibernéticos en Chile, México y Colombia. Un estudio de Derecho Comparado" (Cyber crimes in Chile, Mexico and Colombia. A comparative law study), ISSN: 2594-1356

[209] Diario Oficial de la Federación (10 de junio de 2011). Decreto. Por el cual se modifica la denominación del Capítulo I del Título Primero y reforma diversos artículos de la Constitución Política de los Estados Unidos Mexicanos. Recuperado de http://www.dof.gob.mx/nota_detalle.php?codigo=5194486&fecha=10/06/2011

espionaje, pornografía, delitos en materia de derechos de autor y violación a la intimidad, dejando fuera delitos como fraude y suplantación de personas físicas o jurídico colectivas, entre otros, dado que no ha modificado sus ordenamientos jurídicos.

En este contexto, el Senado de la República exhortó al gobierno mexicano a concluir la etapa de evaluación del marco jurídico vigente para que México se adhiera a la Convención sobre Ciberdelincuencia o convenio de Budapest, ya que tiene más de 10 años analizándolo para proceder a su ratificación.

Siguiendo la línea anterior y, como ejemplo, se tiene el Dictamen con Punto de Acuerdo relativo al Convenio de Budapest sobre Ciberdelincuencia (2019)[210], emitido por la Cámara de Diputados del H. Congreso de la Unión, donde exhorta al titular de la Secretaría de Relaciones Exteriores a impulsar el instrumento de adhesión para que México forme parte del multicitado convenio, argumentando lo siguiente:

> *México ha utilizado el mecanismo de adhesión en nueve tratados impulsados por el Consejo de Europa, incluyendo el Convenio Europeo de Información sobre Derecho Extranjero (ratificado en 2003); el Convenio de Derecho Penal sobre la Corrupción (firmado en 2002), y el Convenio del Consejo de Europa sobre los Delitos Relacionados con los Bienes Culturales (ratificado en 2018), entre otros, los cuales ya han sido ratificados por el Senado mexicano.*

Aunque México mantiene un estatus de “observador”, ha ido más lejos en la regulación de esa temática: es el caso del delito de Pornografía de Personas de Menores de dieciocho años, regulado en el artículo 202 del Código Penal Federal, que guarda relación con el artículo 9. Delitos relacionados con la pornografía infantil del Convenio de Budapest; de la misma manera, el artículo 424 bis, fracción II, de los delitos en materia de Derechos de autor del mismo Código, establece: “A quien fabrique con fin de lucro un dispositivo o sistema cuya finalidad sea desactivar los dispositivos electrónicos de protección de un programa de computación”, tiene

[210] Cámara de Diputados de los Estados Unidos Mexicanos (2019). Dictamen con Punto de Acuerdo. Relativo al Convenio de Budapest sobre Ciberdelincuencia. Comisión de Relaciones Exteriores. Recuperado de http://www5.diputados.gob.mx/index.php/esl/content/download/168058/838814/file/9e_Art_72_Fr_IX_LVotpropoBudap.pdf

relación con el artículo 10. Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines del citado Convenio de Budapest.

Cabe destacar que los últimos avances en materia de regulación sobre delitos cibernéticos fueron el 1° de junio de 2021 con la "Ley Olimpia", publicada en el Diario Oficial de la Federación, la cual trajo consigo un entramado de reformas en materia de delitos cibernéticos al Código Penal Federal y a la Ley General de Acceso de las Mujeres a una Vida Libre de Violencia (2007).

En el caso del Código Penal, se adicionó el Capítulo II, Violación a la Intimidad, al Título Séptimo bis "delitos contra la Indemnidad de Privacidad de la Información Sexual", cuya finalidad es la de tipificar todas aquellas conductas que divulguen contenido íntimo sexual de una persona que tenga la mayoría de edad sin su consentimiento, esto puede ser en cualquier tipo de plataforma digital o red social. Por otra parte, la reforma realizada a la Ley General de Acceso de las Mujeres a una Vida Libre de Violencia cuya finalidad, de acuerdo con Jesika Velázquez (2020)[211], es "reconocer y sancionar la violencia digital y la violencia mediática contra las mujeres, figuras que serán aplicables en todo el país" (párr. 10).

Hay que destacar que es una innovación por parte del Estado mexicano, puesto que en los parámetros del convenio de Budapest solo se sanciona el delito de pornografía con menores de edad, mientras que, con el delito de Violencia a la Indemnidad Sexual, se protege a toda persona que tenga la mayoría de edad y a quienes se divulgue contenido íntimo sexual sin su consentimiento; dicho bien jurídico a proteger está comprendido en el Convenio de Budapest, puesto que todas las personas, mayores o menores de edad, son susceptibles de padecer la difusión de su contenido íntimo sexual sin consentimiento.

Ahora bien, cabe señalar que México es *"una república compuesta por estados libres y soberanos en todo lo concerniente a su régimen interior*" (Art. 40, CPEUM[212]), de esta manera, tanto la federación como sus estados están facultados para legislar, debido a la división de poderes y del sistema de pesos y contra pesos del sistema que lo conforma, algunos estados se han adelantado en la regulación de

[211] VELÁZQUEZ, JÉSIKA. (09 de diciembre de 2020). Ley Olimpia. Instituto de Investigaciones Jurídicas de la Universidad Nacional Autónoma de México. Recuperado de https://revistas.juridicas.unam.mx/index.php/hechos-y-derechos/article/view/15277/16356

[212] Constitución Política de los Estados Unidos Mexicanos, modificada el 29 de Enero de 2016.

los delitos cibernéticos como sucede en el estado de México, la Ciudad de México, estado de Colima, entre otros, con la Ley Ingrid, que de acuerdo con la Secretaría de Gobernación (2020), en su Ficha Técnica señala: La "Ley Ingrid" al igual que la "Ley Olimpia" no se refiere a una ley como tal, sino a un conjunto de reformas legislativas que buscan evitar la exposición de las personas ante los medios para proteger la intimidad y dignidad de las víctimas y sus familiares, combatir la violencia mediática de género y su normalización; sancionando a las personas y servidores públicos que realicen dichas conductas.

En ese mismo orden de ideas tenemos al estado de Jalisco, con la reforma a su Código Penal (1982) registrada el 01 de noviembre de 2021, en su artículo 143 quater, que tipifica el delito de suplantación de identidad por cualquier medio.

4.3.1.9. España y el Convenio sobre la Ciberdelincuencia de Budapest

España, a diferencia del resto de los países analizados, pertenece a la Comunidad Europea, por lo que ha formado parte desde hace más años. De hecho, ha realizado su declaración sobre el Convenio de Cibercrimen de Budapest, considerándose consignada en el instrumento de ratificación depositado el 3 de junio de 2010.

En relación a la aplicación del mismo y entre las reservas realizadas España ha formulado que:

"Para el caso de que el presente Convenio sobre la Ciberdelincuencia sea extendido por el Reino Unido a Gibraltar, el Reino de España desea formular la siguiente declaración:

1. Gibraltar es un territorio no autónomo de cuyas relaciones exteriores es responsable el Reino Unido y que está sometido a un proceso de descolonización de acuerdo con las decisiones y resoluciones pertinentes de la Asamblea General de las Naciones Unidas.

2. Las autoridades de Gibraltar tienen un carácter local y ejercen competencias exclusivamente internas que tienen su origen y fundamento en la distribución y

atribución de competencias efectuadas por el Reino Unido, de conformidad con lo previsto en su legislación interna, en su condición de Estado soberano del que depende el citado territorio no autónomo.

3. En consecuencia, la eventual participación de las autoridades gibraltareñas en la aplicación del presente Convenio se entenderá realizada exclusivamente en el marco de las competencias internas de Gibraltar y no podrá considerarse que produce cambio alguno respecto de lo previsto en los dos párrafos precedentes."

De acuerdo con los artículos 24 y 27 del Convenio, España declara que la autoridad central designada es la Subdirección General de Cooperación Jurídica Internacional del Ministerio de Justicia.

De acuerdo con el artículo 35 del Convenio, España declara que la autoridad central designada es la Comisaría General de Policía Judicial del Ministerio del Interior.

El Convenio comenzó a regir con efectos sobre España a partir del 1º de Octubre de 2010.

4.3.2. Proyecto de Convención Internacional Integral sobre la Lucha contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos (ONU)

4.3.2.1. Breve cronología del Proyecto

Para entender la situación actual de este proyecto, es importante comprender el recorrido que se ha realizado hasta el momento, por lo que destacamos el desarrollo realizado por la Electronic Frontier Foundation (EFF)[213], organización internacional dedicada a la protección de los derechos humanos, que ha seguido de cerca el avance de dicha Convención.

[213] RODRIGUEZ, Katitza y GUILLO, Karen, "Cronología del Tratado de la ONU sobre Ciberdelincuencia"; Url: "https://www.eff.org/es/deeplinks/2023/04/un-cybercrime-treaty-timeline

En Octubre de 2017 la Federación Rusa presenta una carta[214] a la Asamblea General de la ONU con un borrador de la Convención de las Naciones Unidas sobre Cooperación en la Lucha contra la Ciberdelincuencia, destinada a ser distribuida a los Estados miembros.

Dos años después, en Noviembre de 2019, se aprueba en la Asamblea General de la ONU una resolución, patrocinada por Rusia -junto con Bielorrusia, Camboya, China, Irán, Myanmar, Nicaragua, Siria y Venezuela- para crear una convención internacional de lucha contra la ciberdelincuencia. Estados Unidos, la UE y otros países se opusieron a la resolución[215].

Organizaciones de derechos humanos, entre ellas la Asociación para el Progreso de las Comunicaciones y EFF, instaron a la Asamblea General a votar en contra de la resolución, alegando que "podría socavar el uso de Internet para ejercer los derechos humanos y facilitar el desarrollo social y económico"[216].

En Diciembre de 2019, la Asamblea General de la ONU adopta una resolución para crear un Comité Ad Hoc (AHC) encargado de redactar una Convención de la ONU[217] "sobre la lucha contra la utilización de las tecnologías de la información y la comunicación con fines delictivos". La participación en el AHC está abierta a todos los Estados miembros del mundo, así como a observadores de Estados no miembros (como la UE y el Consejo de Europa), la sociedad civil y organizaciones no gubernamentales (ONG) en diversos grados. La Oficina de las Naciones Unidas contra la Droga y el Delito (ONUDD), a través de la Subdivisión de Delincuencia Organizada y Tráfico Ilícito de la División para Asuntos de Tratados, desempeña las funciones de Secretaría del Comité Especial. Sin embargo, la oportunidad de este esfuerzo fue controvertida, ya que otra Resolución de la Asamblea General[218] de la ONU había planteado la preocupación de que las leyes sobre ciberdelincuencia "*en algunos casos se utilizan indebidamente para atacar a los defensores de los*

[214] UNITED NATIONS, Digital Library: Url: https://digitallibrary.un.org/record/1327693?ln=en
[215] AP News: "UN gives green light to draft treaty to combat cybercrime", Url: https://apnews.com/article/79c7986478e5f455f2b281b5c9ed2d15
[216] Carta abierta enviada: Url: https://www.apc.org/sites/default/files/Open_letter_re_UNGA_cybercrime_resolution_0.pdf
[217] UNITED NATIOS, Url: https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home
[218] Documentos Nacioanes Unidas: Url: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N19/427/11/PDF/N1942711.pdf?OpenElement

derechos humanos o han obstaculizado su labor y puesto en peligro su seguridad de manera contraria al derecho internacional".

En 2021, la organización internacional Human Rights Watch manifiesta preocupación sobre que los Estados miembros de la ONU estén iniciando el proceso para un tratado sobre ciberdelincuencia cuyos "paladines son algunos de los gobiernos más represivos del mundo", por lo que declaran que la iniciativa suscita serias preocupaciones en materia de derechos humanos".

El AHC convoca la sesión inaugural de organización, en la que representantes de más de 160 países acuerdan un esquema y las modalidades de las negociaciones. El CSA convoca al menos seis sesiones de negociación de 10 días de duración cada una a partir de 2022, que se celebrarán en Nueva York y Viena. La Asamblea General aprueba la propuesta en medio de las quejas[219] del Reino Unido y otros países de que no se consultó a los Estados miembros sobre el texto final y de que el proceso de redacción careció de inclusividad.

Muchos oradores plantearon objeciones similares, y varios discrepan sobre la estructura de toma de decisiones del CSA. Para fijar los términos de las negociaciones, Brasil presentó una enmienda que exigía que el comité obtuviera la aprobación de una mayoría de dos tercios de los representantes, en lugar de la mayoría simple favorecida por Rusia, "antes de lo cual el Presidente informará al Comité de que se han agotado todos los esfuerzos para llegar a un acuerdo por consenso". La enmienda fue aprobada por 88 votos a favor, 42 en contra y 32 abstenciones. En otra decisión icónica que buscaba una mayor transparencia e inclusión, los Estados miembros aprobaron una lista de representantes[220] para participar en los trabajos del CSA procedentes de instituciones académicas relevantes, el sector privado y ONG como EFF, Eticas, Red en Defensa de los Derechos Digitales, Global Partners Digital, Hiperderecho e Instituto Panameño de Derecho y Nuevas Tecnologías, entre otras. También pueden asistir ONG con estatus consultivo ECOSOC, como Privacy International, Human Rights Watch y Derechos Digitales.

[219] Prensa Naciones Unidas: Url: https://press.un.org/en/2021/ga12328.doc.htm
[220] UNITED NATIONS; Url: https://documents-dds-ny.un.org/doc/UNDOC/GEN/V22/011/91/pdf/V2201191.pdf

Las presentaciones de los Estados miembros en la primera sesión demuestran una pronunciada falta de consenso sobre lo que constituye un "ciberdelito" y el alcance que tendrá el tratado. Estados como Brasil[221], la República Dominicana, la Unión Europea (UE)[222], Liechtenstein, Noruega, Suiza, el Reino Unido y EE.UU. abogan por un enfoque más limitado de los delitos, advirtiendo contra el uso de este tratado para imponer controles más amplios en Internet. Algunos Estados también han pedido la inclusión de delitos relacionados con el contenido, como la incitación al terror (China, Rusia), la desinformación (China, Indonesia) y la violación de los derechos de autor (Indonesia, Liechtenstein, México, Noruega, Rusia, EE.UU.).

En Marzo de 2022, se celebra en Viena la primera consulta intersesional con organizaciones de derechos y otras partes interesadas. Durante una mesa redonda ante los Estados miembros de la ONU, ARTICLE 19[223] expresa su preocupación por la necesidad de una convención sobre ciberdelincuencia y los riesgos de que la convención perpetúe los abusos existentes de las leyes sobre ciberdelincuencia. La ONG AccessNow pide[224] que se eviten los enfoques excesivamente expansivos de la penalización. Desde el hemiciclo, la EFF hace hincapié en la importancia de dar prioridad a la protección de los derechos humanos[225], ya que no hacerlo puede tener consecuencias nefastas, y subraya que el ámbito de aplicación de la convención debería limitarse exclusivamente a los asuntos penales.

En Mayo de 2022, se lleva adelante la segunda sesión de negociación celebrada en Viena. El Comité Ad Hoc solicita la opinión de diversas partes interesadas sobre el texto propuesto para los capítulos del tratado relativos a la penalización, las disposiciones generales, las medidas procesales y la aplicación de la ley. EFF, Privacy International y Human Rights Watch presentan una declaración[226]

---

[221] UNITED NATIONS; Url: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/Comments/Brazil_AHC_Brazilian_Position.pdf

[222] UNITED NATIONS; Url: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/Comments/EU_Position_for_AHC_first_session.pdf

[223] UNITED NATIONS; Url: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_intersessional_consultation/A19_presentation.pdf

[224] UNITED NATIONS; Url: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_intersessional_consultation/Access_Now.pdf

[225] EFF; Url: https://www.eff.org/files/2022/03/02/eff-09-intervention-scope-03022021-vf_0.pdf

[226] UNITED NATIONS; Url: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/EFF_contribution.pdf

al CCA en la que subrayan la importancia de incluir en el tratado sólo los ciberdelitos fundamentales y evitar disposiciones demasiado amplias. Durante una declaración oral ante los Estados miembros de la ONU, EFF, Privacy International y Human Rights Watch reiteraron la necesidad de centrarse en los delitos dirigidos específicamente contra las tecnologías de la información y la comunicación (TIC). La EFF definió los ciberdelitos principales como delitos en los que las TIC sirven tanto de objeto directo como de instrumento de los delitos.

Entre los temas que son de interés de este autor, destacamos que los grupos también piden[227] que cualquier tratado futuro garantice que las disposiciones relativas al acceso ilegal, ilícito o no autorizado a las TIC no penalicen la investigación en materia de seguridad, el trabajo de los denunciantes y otros usos novedosos e interoperables de la tecnología que, en última instancia, benefician al público.

En Junio de 2022 se celebra en Viena la segunda consulta entre periodos de sesiones con múltiples partes interesadas. Antes de la reunión, la EFF expresa su preocupación[228] por el hecho de que algunos Estados miembros de la ONU propongan disposiciones ambiguas para combatir la incitación al odio, el extremismo o el terrorismo, lo que podría poner en grave peligro la libertad de expresión. Por ejemplo, Jordania propone utilizar el proyecto de tratado para penalizar "la incitación al odio o las acciones relacionadas con el insulto a religiones o Estados utilizando redes de información o sitios web", mientras que Egipto pide prohibir "la propagación de la discordia, la sedición, el odio o el racismo". Rusia, en colaboración con Bielorrusia, Burundi, China, Nicaragua y Tayikistán, propuso tipificar una serie de delitos relacionados con el contenido, incluidos actos relacionados con el extremismo vagamente definidos. La ambigua terminología empleada podría dar lugar a interpretaciones excesivamente amplias, que en muchos casos incumplirían las normas de derechos humanos en materia de libertad de expresión.

[227] EFF: Url: https://www.eff.org/deeplinks/2022/07/privacy-international-and-electronic-frontier-foundations-statement-unauthorized

[228] EFF: Url: https://www.eff.org/deeplinks/2022/06/speech-related-offenses-should-be-excluded-proposed-un-cybercrime-treaty

La Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (ACNUDH) subrayó que cualquier futuro tratado sobre ciberdelincuencia no debería incluir delitos basados en el contenido de la expresión en línea[229], afirmando que "*las leyes sobre ciberdelincuencia se han utilizado para imponer restricciones excesivamente amplias a la libertad de expresión al penalizar diversos contenidos en línea, como el extremismo o la incitación al odio*".

En Agosto de 2022 se lleva adelante la tercera sesión de negociación, esta vez realizada en Nueva York. A pesar de que el Convenio se refiere a la ciberdelincuencia, algunos Estados sostienen que debería servir de base para la cooperación internacional en la obtención de pruebas para cualquier delito que se esté investigando. La UE, por ejemplo, propuso un texto de compromiso, afirmando que sigue abierta al concepto de cooperación aplicable a la recogida de pruebas no solo en delitos graves, sino en cualquier delito -una disposición del Convenio de Budapest- siempre que se establezcan sólidas salvaguardias de los derechos humanos.

Brasil[230] y Rusia por su parte sugirieron que la cooperación podría incluir la asistencia mutua para investigaciones y procesamientos en casos "civiles y administrativos" y otras investigaciones de "actos ilícitos" no definidos.

En Noviembre de 2022, se lleva adelante la tercera consulta entre sesiones con múltiples partes interesadas celebrada en Viena. Tras el periodo entre sesiones, el CSA publica el Documento de Negociación Consolidado (DNC)[231], un borrador de texto de las disposiciones del convenio propuestas por los Estados miembros.

El borrador consta de tres capítulos, que comienzan con una declaración de intenciones y terminan con disposiciones sobre cuestiones procesales y de aplicación de la ley, de forma similar al modelo de Budapest.

---

[229] UNITED NATIONS; Url: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/OHCHR_17_Jan.pdf

[230] UNITED NATIONS; Url: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Third_session/Documents/Submissions/Brazil_AHC3.pdf

[231] UNITED NATIONS; "Consolidated negotiating document on the general provisions and the provisions on criminalization and on procedural measures and law enforcement of a comprehensive international convention on countering the use of information and communications technologies for criminal purposes", Url: https://documents-dds-ny.un.org/doc/UNDOC/GEN/222/255/1E/PDF/2222551E.pdf

El segundo capítulo trata de las medidas penales que deben adoptarse a nivel nacional, y se divide en 11 "grupos". Los grupos tratan de delitos, como el acceso ilegal a un sistema informático y el uso indebido de dispositivos, y de procedimientos, como la recogida de datos en tiempo real y la interceptación de datos de contenido.

En Diciembre de 2022, la EFF y otras 10 organizaciones de la sociedad civil escriben a la AHC, en una carta[232] apoyada por docenas de otros grupos y académicos de todo el mundo, expresando su grave preocupación por que la CDN "corre el riesgo de entrar en conflicto con el derecho internacional de los derechos humanos". La carta recomienda una serie de revisiones y modificaciones de la CDN para abordar disposiciones preocupantes que podrían llevar a los Estados miembros a tratar diversos tipos de discurso -muchos de los cuales estarían plenamente protegidos por el derecho internacional de los derechos humanos- como un delito penal. Además, la carta afirma que los delitos cibernéticos básicos del texto impondrían algunas restricciones que podrían interferir con los métodos de trabajo esenciales de periodistas, denunciantes e investigadores de seguridad, por lo que deben revisarse.

La EFF y Privacy International presentan comentarios[233] solicitando que los Estados miembros incluyan controles y equilibrios sólidos en el proyecto de Tratado para alinearlo con la jurisprudencia existente de los tribunales y organismos de derechos humanos. Por ejemplo, el proyecto de texto debería incorporar los principios de legalidad, necesidad y proporcionalidad, y exigir una autorización previa independiente (preferiblemente judicial), una supervisión independiente posterior y el derecho a un recurso efectivo. La EFF y Privacy International también piden salvaguardias que garanticen que las facultades de investigación enumeradas en el Convenio se lleven a cabo de manera que no comprometan la seguridad de las comunicaciones y los servicios digitales.

[232] EFF; "Letter to the UN Ad Hoc Committee to Elaborate a Cybercrime Treaty - Fourth Session"; Url: https://www.eff.org/deeplinks/2022/12/letter-un-ad-hoc-committee

[233] UNITED NATIONS; "Privacy International and Electronic Frontier Foundations' Comments on the Consolidated Negotiating Document of the UN Cybercrime Treaty", Url: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/4th_Session/Documents/Multi-stakeholders/PI-EFF_comments_on_consolidated_text_December_2022.pdf

En Enero de 2023 se lleva a cabo la Cuarta sesión de negociación del Comité Ad Hoc (AHC) celebrada en Viena, con la asistencia de representantes de 149 Estados miembros de la ONU. Durante las negociaciones, gran parte del debate sobre el capítulo de penalización se centró en los delitos relacionados con el contenido de los grupos 5 y 7. La Presidencia de la AHC adoptó un enfoque proactivo para abordar las cuestiones más polémicas.

El material más polémico se encuentra en los grupos 3, 6, 8 y 9. Los delitos propuestos en estos grupos son los siguientes Los delitos propuestos en estos grupos abarcan una amplia gama de conductas para las que no existe un consenso unificado sobre cómo deben definirse, desde la "infracción de los derechos de autor", la "incitación o coacción al suicidio" y la "incitación a la subversión", hasta el "terrorismo", el "extremismo" y el "tráfico de drogas", así como la interceptación de contenidos, la interceptación en tiempo real y la administración de pruebas electrónicas, entre otros.

Durante las negociaciones, varios países, entre ellos Singapur, Malasia y Rusia, pretenden suprimir el artículo 42, que establece salvaguardias esenciales de los derechos humanos frente a los poderes de vigilancia.

En Marzo de 2023 se lleva adelante la cuarta consulta intersesional celebrada con múltiples partes interesadas en Viena y en línea, con la asistencia de 61 Estados miembros y Estados observadores no miembros.

Durante una mesa redonda titulada "Cooperación eficaz y receptiva y otros aspectos del capítulo sobre cooperación internacional", un panelista de INTERPOL cuestionó la eficacia de los tratados de asistencia judicial recíproca (MLAT), citando procesos burocráticos en múltiples jurisdicciones y limitaciones de recursos.

En respuesta a las preocupaciones de INTERPOL, la sociedad civil ha expresado sus reservas sobre su enfoque. Como se afirma en el Principio 12 de los Principios Necesarios y Proporcionados, respaldado por más de 400 ONG: "*Cuando los Estados soliciten asistencia con fines policiales, deberá aplicarse el principio de doble incriminación. ... Los Estados no podrán utilizar los procesos de asistencia judicial recíproca y las solicitudes extranjeras de Información Protegida para eludir las restricciones legales nacionales en materia de Vigilancia de las Comunicaciones.*"

4.3.2.2. Observaciones sobre el tratado

Por la naturaleza de los debates que hemos visto alrededor de este tratado, consideramos que de llegarse a adoptar la sanción de este tratado, tendrá un impacto significativo en la forma en que se regula e investiga el delito cibernético en todo el mundo.

Más adelante en esta tesis, en este mismo Capítulo, realizamos un cuadro comparativo donde se pueden apreciar las diferencias (en algunos casos más, en otras menos) entre las regulaciones propuestas de este tratado, en relación a las ya vigentes por el Convenio de Budapest, tanto a nivel formal como material.

Adherimos a la postura de darle importancia a su regulación, entendiendo que debemos prestar atención a su regulación, toda vez que el tratado puede ofrecer una justificación para prácticas abusivas y permitir a los gobiernos criminalizar y procesar la expresión y el disenso legítimos.

Incluso si su alcance es limitado, es probable que el tratado aumente la capacidad de vigilancia policial transfronteriza, el acceso y el intercambio de datos de las personas.

Entendemos que existe un riesgo real de que no incluya salvaguardias efectivas y sólidas para respetar y proteger el derecho a la privacidad y otros derechos fundamentales.

4.4. Metodología y alcance del estudio

Tratando de aprovechar los aciertos de la investigación realizada a nivel mundial, y con muchos menos recursos y ambiciones, intentaremos replicar parte del estudio teniendo por destino, la actualización sobre la situación normativa en delitos informáticos en los países alcanzados, teniendo en consideración los instrumentos internacionales antes analizados.

En cuanto a la metodología, se ha trabajado inicialmente en la recolección de la legislación aplicable en los países incluídos en el alcance del presente estudio, más

precisamente de los siguientes países que se detallan a continuación por orden alfabético: Argentina, Brasil, Colombia, España y México.

A modo de fuente principal, se ha utilizado como recurso de normativas la biblioteca digital del Departamento de Cooperación Jurídica dependiente de la Secretaría de Asuntos Jurídicos, de la Organización de los Estados Americanos[234], en la cuál existe un Portal Interamericano de Cooperación en Materia de Delito Cibernético. Si bien este portal ha sido un punto de partida, en la mayoría de los países se ha consultado de forma independiente -utilizando buscadores normativos- los textos completos de las normas especiales.

En cada uno de los países se ha consultado y analizado la normativa específica (en caso de existir) y en sus códigos penales vigentes, ya que variadas ocasiones, aún no existiendo una legislación especial o reforma dedicada a la materia, se encontraron que los delitos analizados pueden ser sancionados por los tipos penales "clásicos".

Como consecuencia de este trabajo, se construyó un cuadro de situación con una breve descripción del marco jurídico encontrado en cada país, los que han sido condensados en la Tabla Nº 1 expuesta dentro del apartado de los resultados.

Posteriormente, se ha realizado un análisis de cada una de esas normativas, configurando la realización de un cuadro comparativo que permite identificar a los países que poseen sanción penal para determinadas acciones delictivas informáticas.

Como veremos más adelante, son determinadas, puesto que si bien el trabajo completo incluye el relevamiento de la normativa penal, cada país ha regulado las figuras penales con criterios -incluso con denominaciones diferentes-.

Una vez realizado dicho estudio, podrá finalmente realizarse un análisis comparativo sobre los países alcanzados, determinando los delitos informáticos más

[234] ORGANIZACIÓN DE ESTADOS AMERICANOS, Departamento de Cooperación Jurídica, Portal Interamericano de Cooperación en Materia de Delito Cibernético Url: http://www.oas.org/juridico/spanish/cybersp.htm

receptados penalmente, los países con mejor "calificación" desde el punto de vista penal, entre otra serie de conclusiones que serán posible obtener.

4.5. Identificación de marcos normativos aplicables

Comenzaremos aquí a realizar la primera etapa de la investigación sobre derecho comparado, determinando en cada uno de los países que forman parte del estudio la legislación vigente y pertinente en materia de delitos informáticos, junto a un breve resumen de las observaciones realizadas sobre el marco jurídico aplicable.

4.5.1. Tipos de marcos jurídicos

En primer lugar, -y en los términos de la presente tesis- consideraremos que tienen un tipo de normativa "especial" a aquellos países que, siguiendo el modelo del Convenio de Budapest, incluyen todos o la mayoría de estos aspectos en su regulación:

- Glosario de términos utilizados
- Principios aplicables (por ejemplo, jurisdicción)
- Regulación penal material (o sustantiva) - En el mejor de los casos, clasificados de acuerdo al bien jurídico afectado.
- Regulación de procesal penal (o adjetiva)
- Creación de órgano o estructura estatal encargada de investigación

El ejemplo de un país con una norma especial -al menos al criterio de este autor- puede ser República Dominicana o Nicaragua (aunque no se encuentren en el alcance de este estudio, servirán como referencia), quienes poseen una ley que en su interior regula una parte general, conteniendo algunos principios y conceptos, y posteriormente tipifica los delitos informáticos según el bien jurídico afectado.

Además, incluye un capítulo dedicado al aspecto procesal penal, así como en la propia normativa genera un órgano encargado de la recepción de denuncias, investigación y persecución de los delitos informáticos.

En segundo lugar, definiremos que tienen un tipo de normativa de "actualización" a aquellos países que, en la búsqueda de adaptación y aggiornamiento penal de sus respectivos marcos jurídicos, han optado por el modelo de agregar nuevos tipos penales sueltos al código penal vigente, o bien, modificar tipos penales existentes (de delitos tradicionales) para que puedan ser aplicables a las conductas de los ciberdelitos.

En tercer lugar, definiremos que tienen un tipo de normativa "nula" aquellos países que, por distintos motivos políticos y socioculturales, no disponen -al menos hasta el momento de la redacción de estas líneas en el año 2022- de alguna legislación que incluya o considere la punición penal de los ciberdelitos.

Es decir, de acuerdo a lo explicado anteriormente, las categorías generadas para clasificar los marcos jurídicos identificados serán:

1. Especial
2. Actualización
3. Nula

No obstante y a modo de aclaración interpretativa de los resultados aquí expuestos, debe el lector considerar que el hecho de no haberse encontrado normativa especial regulada sobre los delitos informáticos en algún país, no implica necesariamente que todas las conductas disvaliosas realizadas a través de medios informáticos puedan realizarse en ese país, sin ningún tipo de sanción.

Por un lado, porque pueden existir sanciones de otro tipo que no impliquen normas penales. Por otro, porque las propias normas penales pueden no ser especiales, y aún así pueden seguir aplicándose al caso concreto.

Para desarrollar este segundo punto, debemos tener en consideración el nivel de técnica legislativa que posee dicho país, toda vez que dependiendo de la forma y técnica utilizada en su normativa penal, en el caso que el bien jurídico protegido sea

el mismo, para algunos casos es posible que puedan seguir considerándose aplicables normas penales tradicionales.

4.5.2. Relevamiento de normativas aplicables

País	Legislación	Características Generales	Categoria
Argentina	Código Penal, Ley 26.388 (2008), Ley 25.326 (2000) Ley 26.904 (2013) Ley 27.411 (2017) Ley 27.436 (2018)	A partir de Junio de 2008, la Ley 26.388 conocida como la "ley de delitos informáticos" ha incorporado y realizado una serie de modificaciones al Código Penal argentino. Dicha norma misma no regula este tipo de delitos en un cuerpo normativo separado del Código Penal (CP) con figuras propias o independientes, sino que modifica, sustituye e incorpora figuras típicas a diversos artículos del CP actualmente en vigencia. Se modificó el Epígrafe del Capítulo III cuyo nuevo título es "Violación de Secretos y de la Privacidad", Los artículos que modifica o agrega son: 128, 153, 153 bis, 155, 157, 157 bis, 173, 183, 184, 197, 255. El art. 157 bis ya había sido incorporado por la Ley 25.326 de Protección de Datos Personales (2000) pero fue modificado por la Ley 26.388. En el año 2013, la Ley 26.904 agrega la tipificación de la figura del "grooming" en el art. 131 CP (recibiendo severas críticas por su redacción). En el año 2018, la Ley 27.436 modifica la tipificación del art. 128 CP, incorporando la tipificación a la tenencia simple de material de abuso sexual infantil.	Actualización
Brasil	Ley 12.737 (2012), Ley 11.829 (2008) Ley Nº 14.155, (2021)	La Ley 12.737 es una ley del año 2012, en la cuál se dispone la tipificación criminal de los delitos informáticos y otras providencias. En su regulación incorpora modificaciones para los artículos 154-A, 154-B, 266 y 298. Por su parte, la Ley 11.829 regula el Estatuto de la Niñez y la Adolescencia, para mejorar la lucha contra la producción, venta y distribución de pornografía infantil, así como tipificar como delito la adquisición y posesión de dicho material y otros comportamientos relacionados con la pedofilia en Internet. La Ley 14.155 modificó (aumentando) las penas de muchos de los delitos cibernéticos.	Actualización
Colombia	Ley 1.273 (2009),	La ley 1.273, de sanción legislativa en el año 2009, modifica el Código Penal, creando un nuevo bien jurídico	Actualización

	Ley 1366 (2009)	tutelado denominado "de la protección de la información y de los datos". Se afirma que dicha normativa busca preservar integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones. A través de esta incorporación, suma el CAPÍTULO I, titulado "De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos", a partir del cuál regula una serie de artículos penales que van desde el artículo 269A hasta el artículo 269J. Adicionalmente se incorpora el artículo 58, considerando como agravante general "si la realización de alguna de las conductas punibles, se realicen utilizando medios informáticos, electrónicos o telemáticos".	
México	Código Penal Federal	Mediante reformas se crearon en el Código Penal Federal, dentro del Libro Segundo, Título Noveno - Revelación de Secretos y Acceso Ilícito a Sistemas y Equipos de Informática, los artículos 211 bis 1 al 211 bis 7, que buscaron tipificar los delitos informáticos clásicos (para el año de su incorporación). También se encuentran algunas figuras penales aplicables dentro del Libro Segundo, Título Quinto - Delitos en Materia de Vías de Comunicación y Correspondencia, Capítulo I - Ataques a las Vías de Comunicación y Violación de Correspondencia. Más allá de la tipificación a nivel federal, por la división de potestades entre los diferentes Estados Mexicanos, cada uno de ellos posee su propio código penal (similar a EEUU), existiendo diferencias normativas entre ellos que no podrán ser abordadas en el presente trabajo. Es importante destacar, que algunos Estados Mexicanos tienen además sus propias normas penales, incorporando otros delitos informáticos no analizados en este trabajo.	Actualización
España	Código Penal	España posee su código penal regulado a través de su Ley Orgánica 10/1995, de 23 de noviembre. Dicha ley, es modificada por normativas posteriores, que van haciendo sus actualizaciones al Código, tal como lo realizó la Ley Orgánica Ley Orgánica 1/2015, de 30 de marzo, a través de la cuál se realizaron diversas actualizaciones al artículo 197 que contiene varios delitos informáticos, así como al artículo 264.	Actualización

Tabla Nº 1: Legislación vigente en materia de delitos informáticos en los países incluídos en el estudio

En esta Tabla Nº 1 se ha podido concentrar la primera etapa de los resultados, indicándose por país, la legislación vigente y pertinente en materia de delitos informáticos, junto a un breve resumen de las observaciones realizadas sobre el marco jurídico aplicable.

Como puede observarse, al momento de la realización de la búsqueda todos los países de nuestro estudio cuentan con alguna normativa que en mayor o menor medida, agregan o tipifican delitos informáticos en su legislación penal, por lo que a nuestro criterio, consideramos que su clasificación era de “actualización”.

A los fines académicos y con la intención de generar una primera aproximación sobre el estado de salud de la normativa alcanzada, realizaremos una clasificación sobre el tipo de normativa encontrada.

4.6. Relevamiento de delitos informáticos tipificados

Resuelta la primera etapa de identificación de las normas vigentes en los países incluídos en el relevamiento, es posible iniciar una segunda fase de análisis más complejo y de mayor profundización a nivel normativo.

Esta fase tiene como punto de partida la construcción de un cuadro de distintos delitos informáticos, que serán el denominador común a fines comparativos sobre el relevamiento que se llevará a cabo en las distintas legislaciones de los países alcanzados.

La necesidad de construcción de este cuadro inicial con determinados delitos “preseleccionados” tiene origen en la gran gama de criterios que han sido adoptados por los países latinoamericanos, que impide encontrar con facilidad una base comparativa que facilite el estudio propuesto.

Es decir, dependiendo de las normativas analizadas, la cantidad de delitos informáticos tipificados difiere no sólo con respecto a las conductas sancionadas, sino también con respecto al contenido (elementos necesarios para considerar que una acción se encuentra penalmente tipificada).

Tenemos que reconocer que la primer versión de este estudio, fue realizada en una investigación durante el año 2013[235] y 2014[236], publicada en dos partes debido a la extensión de la misma. No obstante, la demora en la publicación de la presente tesis, ha obligado que en el año 2022, se vuelva a realizar un repaso y actualización de todo lo realizado, generando la modificación de gran parte de estas líneas.

En este punto es obligatoria y necesaria la referencia de un artículo muy relacionado con esa sección de la investigación, realizado por el maestro Dr. Marcelo Riquert, que en el año 2014 publicó un estudio[237] abordando el plexo normativo regional sudamericano (Mercosur) y el Convenio sobre Cibercriminalidad de Budapest[238].

En su trabajo, el Dr. Riquert avanza con una empresa similar, restringida a los países sudamericanos y teniendo como alcance todos los tipos penales del Convenio de Budapest (art. 2 al art. 10). Adicionalmente al estudio de las figuras penales propiamente dicha, Riquert ha extendido el análisis sumando la investigación sobre tentativa y complicidad (art. 11), Responsabilidad de las personas jurídicas (art. 12) y Sanciones y Medidas (art. 13), temas sobre los cuales ha desarrollado otros trabajos[239] de gran valor.

En nuestro caso, hemos optado por un lado, en incluir casi la totalidad de los delitos incluídos en la parte material del Convenio de Budapest, dejando solamente excluido el artículo 10, que regula aquellas infracciones vinculadas a los atentados a la propiedad intelectual y a los derechos afines.

---

[235] TEMPERINI, Marcelo: “Delitos Informáticos en Latinoamérica: Un estudio de derecho comparado. 1ra. Parte”, Publicación: 1er. Congreso Nacional de Ingeniería Informática / Sistemas de Información. 2013. ISSN: 2346-9927

[236] TEMPERINI, Marcelo: “Delitos Informáticos en Latinoamérica: Un estudio de derecho comparado. 2da. Parte”, Publicación: Simposio de Informática y Derecho. Jornadas Argentinas de Informática Nº 43 - 2014, ISSN: 1850-2814

[237] RIQUERT, Marcelo: “Convenio sobre Cibercriminalidad de Budapest y el Mercosur Propuestas de derecho penal material y su armonización con la legislación regional sudamericana”, Publicado en Revista Derecho Penal. Año III, N° 7 pág. 107, Infojus, Id SAIJ: DACF140393

[238] COUNCIL OF EUROPE. “Convenio de Cibercriminalidad de Budapest”. Budapest, 23 de noviembre de 2001. Url: http://www.coe.int/t/dghl/standardsetting/t-cy/ETS_185_spanish.pdf , Consultado: 27 de Junio de 2017

[239] RIQUERT, M. A. (2018). La responsabilidad penal de las personas jurídicas en Argentina y el Convenio de Budapest. In Cibercrimen II: nuevas conductas penales y contravencionales. Inteligencia artificial aplicada al derecho penal y procesal penal. Novedosos medios probatorios para recolectar evidencia digital. Cooperación internacional y victimología (p. 443). Editorial B de F.

Por otro lado, y buscando no quedar encorsetados en las recomendaciones europeas, nuestro estudio tendrá una mayor amplitud sobre las figuras penales analizadas, adicionando a los delitos del Convenio de Budapest, otros delitos informáticos más específicos cuya importancia ha sido más marcada en los últimos años.

En consecuencia, y teniendo en consideración las limitaciones del alcance que toda investigación académica debe tener, se ha construído una tabla inicial de los delitos informáticos -denominadores comunes- que serán analizados en cada país, a fin de poder llevar adelante la segunda parte de la investigación, incluyendo los siguientes:

Id.	Delito tipificado
1	Acceso ilícito a sistemas o datos informáticos (intrusismo informático)
2	Interceptación ilícita de sistemas o datos informáticos
3	Ataques a la integridad de datos informáticos (cracking)
4	Ataques a la integridad de sistemas informáticos (denegación de servicios)
5	Abuso de dispositivos
6	Falsificación informática
7	Fraude informático
8	Delitos relacionados con el abuso sexual infantil
9	Suplantación de identidad digital
10	Captación ilegítima de datos (Phishing)
11	Violación de datos personales

Tabla Nº 2: Cuadro de delitos informáticos alcanzados por la investigación

Como puede observarse en la construcción de la tabla de delitos informáticos alcanzados, en los primeros lugares (del 1 al 8) se han detallado aquellas figuras penales más clásicas, con los delitos informáticos propios o puros más conocidos y

donde existe un mayor nivel de consenso acerca de la necesidad de su tipificación penal, en concordancia con las recomendaciones del Convenio de Budapest.

Los delitos 9, 10 y 11, se han incluído algunas figuras adicionales, en algunos casos más complejas que, por un lado, se pueden encontrar diferentes proyectos e iniciativas de ley que a la fecha buscan su tipificación y por otro lado, son figuras que se han encontrado tipificadas en algunos de los ordenamientos abordados, siendo útiles a modo comparativo con el resto de los ordenamientos.

Desde un punto de vista organizativo por la cantidad de información, se ha realizado una tabla por cada uno de las figuras penales investigadas, a fin de facilitarle a la persona lectora la comparación del mismo tipo penal, entre los diferentes países.

4.6.1. Cuadro comparativo entre el Convenio de Budapest y el Proyecto de Regulación de la ONU

Basados en los resultados generados en la última tabla, donde hemos identificado los delitos de interés para este estudio, hemos optado por comenzar generando un primera acercamiento hacia estas figuras penales a través de la generación de un cuadro comparativo entre la regulación propuesta por el Convenio de Cibercrimen de Budapest (Consejo de Europa) y el Proyecto de la Convención Internacional Integral sobre la Lucha contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos (ONU).

ID	Convenio Nº 185 del Consejo de Europa (Convenio de Budapest)	Proyecto (Mayo 2023) de Convención Internacional Integral sobre la Lucha contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos
1	**Artículo 2. Acceso ilícito** Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, el acceso doloso y sin autorización a todo o parte de un sistema informático. Los Estados podrán exigir que la infracción sea cometida con vulneración de medidas de seguridad, con la intención de obtener	**Artículo 7: Acceso Ilícito** 1. Cada Estado parte adoptará las medidas legislativas y de otra índole que sean necesarias para tipificar como delito en su derecho interno el acceso deliberado y sin derecho a la totalidad o una parte de un [sistema informático] [dispositivo de tecnología de la información y las comunicaciones]. 2. Los Estados partes podrán exigir como requisito que el delito se cometa infringiendo las medidas de

	los datos informáticos o con otra intención delictiva, o también podrán requerir que la infracción se perpetre en un sistema informático conectado a otro sistema informático.	seguridad, con la intención de obtener [datos informáticos] [información digital] o con otra intención deshonesta, o en relación con un [sistema informático] [dispositivo de tecnología de la información y las comunicaciones] que esté conectado a otro [sistema informático] [dispositivo de tecnología de la información y las comunicaciones].
2	**Artículo 7: Interceptación Ilícita** Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, la interceptación, dolosa y sin autorización, cometida a través de medios técnicos, de datos informáticos --en transmisiones no públicas-- en el destino, origen o en el interior de un sistema informático, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporta tales datos informáticos. Los Estados podrán exigir que la infracción sea cometida con alguna intención delictiva o también podrán requerir que la infracción se perpetre en un sistema informático conectado a otro sistema informático.	**Artículo 7: Interceptación Ilícita** 1. Cada Estado parte adoptará las medidas legislativas y de otra índole que sean necesarias para tipificar como delito en su derecho interno la interceptación deliberada y sin derecho, por medios técnicos, de transmisiones no públicas de [datos informáticos] [información digital] a un [sistema informático] [dispositivo de tecnología de la información y las comunicaciones], desde él o dentro de él, incluidas las emisiones electromagnéticas provenientes de un [sistema informático] [dispositivo de tecnología de la información y las comunicaciones] que transporten [esos datos informáticos] [esa información digital]. 2. Los Estados partes podrán exigir como requisito que el delito se cometa con intención deshonesta o en relación con un [sistema informático] [dispositivo de tecnología de la información y las comunicaciones] que esté conectado a otro [sistema informático] [dispositivo de tecnología de la información y las comunicaciones].
3	**Artículo 4: Atentados contra la integridad de los datos** 1. Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, la conducta de dañar, borrar, deteriorar, alterar o suprimir dolosamente y sin autorización los datos informáticos. 2. Los Estados podrán reservarse el derecho a exigir que el comportamiento descrito en el párrafo primero ocasione daños que puedan calificarse de graves.	**Artículo 8: Interferencia con [datos informáticos] [información digital]** 1. Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su derecho interno todo acto deliberado y sin derecho que dañe, borre, deteriore, altere o suprima [datos informáticos] [información digital]. 2. Los Estados partes podrán exigir como requisito que los actos descritos en el párrafo 1 comporten daños graves.
4	**Artículo 5. Atentados contra la integridad del sistema** Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal,	**Artículo 9. Interferencia con un [sistema informático] [dispositivo de tecnología de la información y las comunicaciones]** Cada Estado parte adoptará las medidas legislativas y de otra índole que sean necesarias para tipificar como

	conforme a su derecho interno, la obstaculización grave, cometida de forma dolosa y sin autorización, del funcionamiento de un sistema informático, mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos.	delito en su derecho interno la obstaculización grave, deliberada y sin derecho del funcionamiento de un [sistema informático] [dispositivo de tecnología de la información y las comunicaciones] mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de [datos informáticos] [información digital].
5	**Artículo 6. Abuso de equipos e instrumentos técnicos** 1. Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, las siguientes conductas cuando éstas sean cometidas dolosamente y sin autorización: a. la producción, venta, obtención para su utilización, importación, difusión u otras formas de puesta a disposición 1. de un dispositivo, incluido un programa informático, principalmente concebido o adaptado para permitir la comisión de una de las infracciones establecidas en los artículos 2 a 5 arriba citados; 2. de una palabra de paso (contraseña), de un código de acceso o de datos informáticos similares que permitan acceder a todo o parte de un sistema informático, con la intención de utilizarlos como medio para cometer alguna de las infracciones previstas en los artículos 2 a 5; y b. la posesión de alguno de los elementos descritos en los parágrafos (a) (1) o (2) con la intención de utilizarlos como medio para cometer alguna de las infracciones previstas en los artículos 2-5. Los Estados podrán exigir en su derecho interno que concurra un determinado número de elementos para que nazca responsabilidad pena 2. Lo dispuesto en el presente artículo no generará responsabilidad penal cuando la producción, venta, obtención para la utilización, importación, difusión u otras formas de puesta a disposición mencionadas en el párrafo 1 no persigan la comisión de una infracción prevista en los artículos 2 a 5 del presente Convenio, como en el caso de ensayos autorizados o de la protección de un	**Artículo 10. Uso indebido de dispositivos** 1. Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada y sin derecho de los siguientes actos: a) la obtención, producción, venta, adquisición para su utilización, importación, distribución o cualquier otra forma de puesta a disposición de: i) cualquier dispositivo, incluido un programa, concebido o adaptado principalmente para la comisión de alguno de los delitos tipificados con arreglo a los artículos 6 a 9 de la presente Convención; o ii) una contraseña, credenciales de acceso, firma electrónica o datos similares mediante los cuales se pueda acceder a la totalidad o a una parte de un [sistema informático] [dispositivo de tecnología de la información y las comunicaciones] con la intención de que el dispositivo, la contraseña, las credenciales de acceso o los datos similares se utilicen para cometer alguno de los delitos tipificados con arreglo a los artículos 6 a 9 de la presente Convención; y b) la posesión de alguno de los elementos contemplados en el párrafo 1 a) i) o ii) del presente artículo con intención de que sean utilizados para cometer alguno de los delitos tipificados con arreglo a los artículos 6 a 9 de la presente Convención. Los Estados partes podrán exigir en su derecho interno la posesión de un número determinado de dichos elementos como requisito para que se considere q ue existe responsabilidad penal. 2. No se interpretará que el presente artículo impone responsabilidad penal cuando la obtención, producción, venta, adquisición para la utilización, importación, distribución o cualquier otra forma de puesta a disposición o la posesión mencionada en el párrafo 1 del presente artículo no tenga por objeto la comisión de uno de los delitos tipificados con arreglo a los artículos 6 a 9 de la presente Convención, como en el caso de la realización de pruebas autorizadas o de la protección de

	sistema informático. 3. Los Estados podrán reservarse el derecho de no aplicar el párrafo 1, a condición de que dicha reserva no recaiga sobre la venta, distribución o cualesquiera otras formas de puesta a disposición de los elementos mencionados en el parágrafo 1 (a)(2).	un [sistema informático] [dispositivo de tecnología de la información y las comunicaciones]. 3. Cada Estado parte podrá reservarse el derecho a no aplicar el párrafo 1 del presente artículo, siempre que dicha reserva no esté relacionada con la venta, distribución ni ninguna otra forma de puesta a disposición de los elementos mencionados en el párrafo 1 a) ii) del presente artículo.
6	**Artículo 7. Falsedad informática** Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, la introducción, alteración, borrado o supresión dolosa y sin autorización de datos informáticos, generando datos no auténticos, con la intención de que sean percibidos o utilizados a efectos legales como auténticos, con independencia de que sean directamente legibles e inteligibles. Los Estados podrán reservarse el derecho a exigir la concurrencia de un ánimo fraudulento o de cualquier otro ánimo similar para que nazca responsabilidad penal.	**Artículo 11. Falsificación informática** 1. Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su derecho interno la introducción, alteración, borrado o supresión deliberados y sin derecho de [datos informáticos] [información digital] que genere datos inauténticos con intención de que sean tomados o utilizados como auténticos a efectos legales, con independencia de que los datos sean legibles e inteligibles directamente. 2. Los Estados partes podrán exigir como requisito que exista una intención fraudulenta o deshonesta similar para que se considere que existe responsabilidad penal.
7	**Artículo 8. Estafa informática** Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, la producción de un perjuicio patrimonial a otro, de forma dolosa y sin autorización, a través de: c. la introducción, alteración, borrado o supresión de datos informáticos, d. cualquier forma de atentado al funcionamiento de un sistema informático, con la intención, fraudulenta o delictiva, de obtener sin autorización un beneficio económico para sí mismo o para tercero.	**Artículo 12. Robo o fraude informáticos** Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su derecho interno la provocación deliberada y sin derecho de la pérdida de bienes de otra persona mediante los siguientes actos: a) la introducción, alteración, borrado o supresión de [datos informáticos] [información digital]; b) la interferencia en el funcionamiento de un [sistema informático] [dispositivo de tecnología de la información y las comunicaciones] con la intención fraudulenta o deshonesta de procurar para sí o para otra persona, sin derecho, un beneficio económico o [datos informáticos] [información digital] que contenga[n] datos personales, incluida información relacionada con la cuenta bancaria de una persona, sin el consentimiento de la persona afectada, y a los que de otro modo el autor del acto no tendría acceso.

8	**Artículo 9. Infracciones relativas a la pornografía infantil** 1. Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, las siguientes conductas cuando éstas sean cometidas dolosamente y sin autorización: a. la producción de pornografía infantil con la intención de difundirla a través de un sistema informático; b. el ofrecimiento o la puesta a disposición de pornografía infantil a través de un sistema informático; c. la difusión o la transmisión de pornografía infantil a través de un sistema informático; d. el hecho de procurarse o de procurar a otro pornografía infantil a través de un sistema informático; e. la posesión de pornografía infantil en un sistema informático o en un medio de almacenamiento de datos informáticos. 2. A los efectos del párrafo 1 arriba descrito, la «pornografía infantil» comprende cualquier material pornográfico que represente de manera visual: a. un menor adoptando un comportamiento sexualmente explícito; b. una persona que aparece como un menor adoptando un comportamiento sexualmente explícito; c. unas imágenes realistas que representen un menor adoptando un comportamiento sexualmente explícito. 3. A los efectos del párrafo 2 arriba descrito, el término «menor» designa cualquier persona menor de 18 años. Los Estados podrán exigir un límite de edad inferior, que debe ser como mínimo de 16 años. 4. Los Estados podrán reservarse el derecho de no aplicar, en todo o en parte, los párrafos 1 (d) y 1 (e) y 2 (b) y 2 (c).	**Artículo 13. Delitos relacionados con material en línea que muestra abusos sexuales de niños o explotación sexual de niños** 1. Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada y sin derecho de los siguientes actos: a) producir, ofrecer, vender, distribuir, transmitir, emitir, exhibir, publicar o hacer disponible de otro modo material que muestre abusos sexuales de niños o explotación sexual de niños mediante un [sistema informático] [dispositivo de tecnología de la información y las comunicaciones]; b) solicitar o adquirir material que muestre abusos sexuales de niños o explotación sexual de niños, acceder a él o interactuar con él de otro modo mediante un [sistema informático] [dispositivo de tecnología de la información y las comunicaciones]; c) poseer o controlar material que muestre abusos sexuales de niños o explotación sexual de niños almacenado en un [sistema informático] [dispositivo de tecnología de la información y las comunicaciones] u otro medio de almacenamiento; d) financiar o facilitar los delitos tipificados con arreglo a este artículo o beneficiarse de ellos. 2. A los efectos del presente artículo: a) el término “material que muestre abusos sexuales de niños o explotación sexual de niños” incluirá el material que muestre o represente a un niño o a una persona que parezca ser un niño: i) que participe en actividades o adopte posturas sexuales reales o simuladas; ii) en presencia de una persona que practique cualquier actividad sexual; iii) cuyas partes genitales se exhiban con fines primordialmente sexuales; o iv) que sea, o se dé a entender que es, víctima de torturas o tratos o penas crueles, inhumanos o degradantes, cuando dicho material sea de carácter sexual; b) el término “material” comprenderá imágenes, videos y medios de emisión en directo, material escrito y grabaciones de audio. 3. Los Estados partes podrán exigir como requisito que el material definido en el párrafo 2 b) se limite a material que: a) muestre, describa o represente a un niño real; o b) muestre imágenes de abusos sexuales de niños o explotación sexual de niños. 4. Los Estados partes adoptarán medidas para que no se criminalice a niños por el material descrito en el

		párrafo 2 del presente artículo que generen ellos mismos. 5. Los Estados partes velarán por que existan salvaguardias adecuadas en el derecho interno para proteger a los niños acusados de este delito, en consonancia con sus obligaciones en virtud de la Convención sobre los Derechos del Niño y sus Protocolos.
9	No posee regulación recomendada	No posee regulación recomendada
10	No posee regulación recomendada	No posee regulación recomendada
11	No posee regulación recomendada	No posee regulación recomendada

Tabla Nº 3: Cuadro comparativo de delitos sugeridos por el Convenio de Budapest y el Proyecto de la ONU

A modo de conclusión preliminar sobre este cuadro, podemos mencionar que todas las figuras reguladas en el Convenio de Cibercrimen de Budapest (al menos de las incluídas en este estudio), encuentran también su propuesta de regulación en el Proyecto de Tratado de la ONU, evidenciando que existe un acuerdo general sobre que todas las figuras básicas de Budapest, efectivamente deben ser sancionadas.

Del análisis de las propuestas para regular cada figura penal propiamente dicha, no se encuentran grandes diferencias. Quizás en la regulación de la figura de tenencia o distribución de material de abuso sexual infantil, se puede encontrar regulación con un mayor grado de detalle en el Proyecto de la ONU.

Recordamos por último, que el Tratado propuesto por la ONU, como hemos visto en la sección 4.3.2. aún continúa siendo centro de debates y modificaciones, por lo que las presentes líneas se escriben relacionadas a la versión publicada en Marzo 2023.

4.6.2. Dificultades metodológicas

Antes de comenzar con el desarrollo de cada delito informático en particular, debemos advertir sobre la dificultad metodológica existente al momento de la

realización de la tarea. Nos referimos a que, la diversidad de políticas penales vigentes en cada país, en combinación con la tradición jurídica y técnicas legislativas que cada uno emplea, nos brinda un panorama muy diversos de figuras penales a considerar.

Bajo este contexto, para confirmar si dicha figura penal se encuentra o no efectivamente tipificada, hemos tenido un criterio amplio de aceptación de la misma. Es decir, si la figura penal encontrada tiene o guarda los elementos básicos de la conducta analizada, optamos por considerar una respuesta positiva sobre su inclusión en dicho marco normativo.

Para casos de dudas, y como una forma de evitar caer en los binarios, hemos agregado la posibilidad de indicar que dicha conducta penal se encuentra "parcialmente" incluída. Esta opción intermedia, tendrá utilidad sobre todo para algunas figuras penales complejas, como el caso del delito de abuso de dispositivos (art. 6 del Convenio de Budapest), en el cual se incluyen varias acciones a regular. En el caso de considerar que algunas de las acciones reguladas se encuentren tipificadas, pero no todas, nos inclinaremos por clasificar la parcialidad de su cumplimiento.

En el caso que las conductas encontradas no se ajusten a las categorías de análisis, o bien, no reúnan elementos básicos como para considerar su tipificación penal, optamos por determinar su no regulación en dicho país.

4.6.3. Delito 1: Acceso ilícito a sistemas o datos informáticos

Este primer delito ha sido propuesto como obligatorio en la Convención de Cibercrimen de Budapest en el artículo 2[240] de la Sección 1. Derecho penal material -

[240] "Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, el acceso doloso y sin autorización a todo o parte de un sistema informático. Las Partes podrán exigir que la infracción sea cometida con vulneración de medidas de seguridad, con la intención de obtener los datos informáticos o con otra intención delictiva, o también podrán requerir que la infracción se perpetre en un sistema informático conectado a otro sistema informático

Título 1: Infracciones contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos:

La conducta básica refiere al acceso doloso y sin autorización a todo o parte de un sistema o dato informático. Alternativamente se establecen como elementos del tipo penal: la vulneración de medidas de seguridad; la intención de obtener los datos informáticos o con otra intención delictiva, la realización de un perjuicio como elemento del tipo penal.

De acuerdo al informe explicativo del Consejo de Europa sobre el Convenio de Budapest[241], en su párrafo 46, explican que el término "acceso" abarca la entrada a un sistema informático o a alguna parte del mismo (hardware, componentes, datos almacenados del sistema instalado, directorios, datos relativos al tráfico y datos relacionados con los contenidos). Sin embargo, no incluye el mero envío de un mensaje de correo electrónico o de un archivo a ese sistema. El término "acceso" incluye el ingreso a otro sistema informático, al que esté conectado a través de redes de telecomunicaciones públicas, o a un sistema informático que esté conectado a la misma red, como una LAN (red de área local) o una Intranet (red interna) que opere en el seno de una organización. No tiene importancia el método de comunicación utilizado (por ej., desde lejos, incluidos los enlaces inalámbricos, o desde una corta distancia).

A nivel doctrinario, el acceso sin otros fines o conductas dañosas, lo que se conoce como “mero intrusismo” es motivo de disputa debido al reconocimiento del bien jurídico que se pretende tutelar. En el año 2010[242], postulamos nuestra posición crítica acerca de la tipificación de esta figura en el sistema argentino, entendiendo que el bien jurídico protegido en realidad es la confidencialidad de la información (uno de los tres pilares de la Seguridad de la Información). En el artículo realizamos algunas consideraciones respecto a la postura de su calificación como un delito de peligro, dando lugar a la existencia de situaciones de perfeccionamiento del mismo, sin existencia del daño concreto.

---

[241] Consejo de Europa, STE núm. 185, Informe Explicativo - CONVENIO SOBRE LA CIBERDELINCUENCIA; Disponible en Url: https://rm.coe.int/16802fa403

[242] TEMPERINI, Marcelo; “Delitos Informáticos: La punibilidad del Hacking y sus consecuencias”; Publicación: Simposio de Informática y Derecho. Jornadas Argentinas de Informática Nº 39 - 2010. ISSN: 1850-2814

La segunda crítica que realizamos en ese artículo, consistía en el abuso de la pena de prisión privativa de libertad como sanción a la conducta. Sobre esta línea y muy atinadamente el Dr. Marcelo Riquert sostiene que "*el Convenio admite —no exige—como sanción la pena privativa de libertad. Un problema básico de ésto es que, si en el delito más leve, básico y de aplicación subsidiaria se usa la modalidad más grave de sanción; se caerá en problemas serios de proporcionalidad en el resto de las conductas. En realidad, se trata de un comportamiento sobre el que se discute si realmente es necesaria la intervención del derecho penal o si bastaría con la del contravencional o sancionador administrativo. Se estiman más lógicas las penas pecuniarias o de inhabilitación que la prisión.*"

Como hemos ya analizado en el Capítulo 2 de la presente tesis, existen diferentes posturas sobre la tipificación de esta figura, que de alguna manera, se convierte en la conducta básica o introductoria, a partir de la cual se pueden dar otras figuras más complejas, por lo que remitimos allí.

A modo de adicional, sobre el final del repaso normativo, comentaremos la existencia de un actual movimiento en Argentina que busca la inclusión de una excepción dentro de la figura penal del art. 153 a fin de prevenir la existencia de nuevos casos de investigadores en seguridad de la información, que han sido penalmente perseguidos.

Hecha estas apreciaciones iniciales, sin más preámbulos, comenzamos con el repaso de la tipificación de esta figura en los 5 países que forman parte del estudio:

País	Delito 1: Acceso Ilícito (intrusismo informático)
Argentina	**CP Artículo 153 bis:** Será reprimido con prisión de quince (15) días a seis (6) meses, si no resultare un delito más severamente penado, el que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido.

País	Delito 1: Acceso Ilícito (intrusismo informático)
	La pena será de un (1) mes a un (1) año de prisión cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros. También podría ser aplicable el párrafo 1 del art. 157 bis: (26.388). Artículo 157 bis: Será reprimido con la pena de prisión de un (1) mes a dos (2) años el que: 1. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales;
Brasil	**CP. Art. 154-A.** Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita: Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa. Aumenta-se a pena de 1/3 (um terço) a 2/3 (dois terços) se da invasão resulta prejuízo econômico. § 3o Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido: Pena – reclusão, de 2 (dois) a 5 (cinco) anos, e multa.
Colombia	**CP. Art. 269 A.** El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.
México	**CP. Artículo 211 bis 1**. Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa. Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.

País	Delito 1: Acceso Ilícito (intrusismo informático)
España	**Artículo 197 bis. (1er párrafo).** 1. El que por cualquier medio o procedimiento, vulnerando las medidas de seguridad establecidas para impedirlo, y sin estar debidamente autorizado, acceda o facilite a otro el acceso al conjunto o una parte de un sistema de información o se mantenga en él en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años.

Tabla Nº 4: Cuadro comparativo de tipificación de Delito 1: Acceso Ilícito (intrusismo informático)

4.6.3.1. Movimiento para la despenalización de la actividad de seguridad informática

Como hemos visto anteriormente en el desarrollo cronológico del estudio del Proyecto de regulación de la ONU sobre cibercrimen (sección 4.3.2. de esta tesis), muchas organizaciones de nivel mundial, continúan advirtiendo que el tipo de regulación recomendada tanto por el Convenio de Budapest como el realizado por la propia ONU, avanza en la persecución de algunas actividades que a nuestro criterio, deberían estar exceptuadas de pena.

Argentina no escapa de esa realidad y es por eso que durante el año 2021, desde Ekoparty[243] la Conferencia de Hacking más importante de Latinoamérica, se ha llevado adelante una campaña sobre la despenalización de los investigadores en seguridad de la información, en la cual hemos formado parte desde la conducción de uno de los espacios dedicados a brindar información sobre la normativa vigente a los nuevos profesionales del rubro de la seguridad de la información. Su construcción ha sido resultado de un proceso de colaboración colectivo de abogados, ingenieros informáticos y distintos profesionales de la seguridad de la información.

[243] Organización que desde hace más de 15 años lleva adelante la Conferencia Latinoamericana más importante en materia de seguridad informática

El boceto de proyecto de Ley tiene como objeto tener en consideración la incorporación de un nuevo párrafo al tipo penal del artículo 153 bis, en el que pueda considerarse un párrafo extra que sirva como protección para aquel que como investigador de seguridad, descubre una falla y la reporta.

Dicha protección ha sido pensada como una alternativa legal de exención de la responsabilidad penal de aquellas personas que puedan acreditar que su accionar ha sido en miras de la protección de interés público, o bien, que puedan acreditar que su acción ha sido realizada de buena fe y en el marco de una investigación en seguridad de la información, detecte una falla, error, vulnerabilidad o problemas de seguridad, exigiendo siempre su comunicación al responsable del sistema.

El proyecto reza el siguiente texto:

Incorpórase como tercer párrafo del Artículo 153 bis del Código Penal de la Nación el siguiente:

Estará exento de responsabilidad penal el que hubiere obrado con el propósito inequívoco de proteger un interés público. También quedará exento quien obrando de buena fe y en el marco de una investigación de seguridad de la información, comunicare la vulnerabilidad encontrada al propietario del sistema informático.

Dicho proyecto se ha trabajado postulando que la acción de comunicación del descubrimiento de las vulnerabilidades de seguridad encontradas, serían una prueba de la buena fe en su accionar, tendiente a la cooperación y colaboración en el aseguramiento y protección de los sistemas y datos informáticos.

Entre los fundamentos se afirma que dicha comunicación (la solicitada para la eximición) podría ser probada a través del envío de una comunicación electrónica a los distintos canales de contacto que exhiba el propietario del sistema o los datos informáticos, así como a otras formas que pudieran revelar su intención de dar a conocer los problemas encontrados al responsable del sistema,

Con respecto a demostrar que la acción se encontraba en el marco de una investigación en seguridad de la información, se considera que existen diferentes

formas de acreditar la misma, ya sea haber realizado publicaciones previas de papers o artículos de investigación, así como la posibilidad de demostrar haber brindado charlas o conferencias de seguridad de la información, entre otros elementos o indicios que puedan indicar que la buena fe del sujeto activo.

En relación a la opción de haber obrado en aras de un interés público, se anuncia como ejemplo acciones de investigación y reporte de fallas de seguridad relacionadas a un sistema o dato pertenecientes a un organismo público, donde exista afectación de datos personales de los ciudadanos.

Que, consideramos que la problemática visibilizada tiene relación directa con temáticas que ya han sido advertidas por diversas organizaciones internacionales, así como en diversas declaraciones internacionales al respecto, como en el IGF Berlin 2019[244].

Como cierre de este tema, al momento de escribir estas líneas, la campaña generada en Change.org de recolección de firmas para apoyar dicho proyecto[245], lleva casi 600 firmas.

Al momento de la presentación de esta tesis de doctorado (principios del 2024), se contaba con la información de que dicho proyecto sería presentado formalmente en el Senado de la Nación Argentina durante el mes de Marzo 2024.

4.6.4. Delito 2: Interceptación ilícita de datos informáticos

Propuesto como obligatorio en la Convención de Cibercrimen de Budapest en el artículo 3[246] de la Sección 1. Derecho penal material - Título 1: Infracciones contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos.

---

[244] IGF 2019 BPF on Cybersecurity contributes to UN OEWG, Berlin 2019, Url: https://www.intgovforum.org/multilingual/content/igf-2019-bpf-on-cybersecurity-contributes-to-un-oewg

[245] Change.org: Url: https://www.change.org/p/legisladores-los-investigadores-de-seguridad-no-somos-delincuentes

[246] Artículo 3. Interceptación ilícita: Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la interceptación deliberada e ilegítima, por medios técnicos, de datos informáticos comunicados en transmisiones no públicas efectuadas a un sistema informático, desde un sistema informático o dentro del mismo, incluidas las emisiones electromagnéticas procedentes de un sistema informático que contenga dichos datos informáticos. Cualquier Parte podrá exigir que el delito se haya cometido con intención delictiva o en relación con un sistema informático conectado a otro sistema informático.

Esta figura penal es intermedia, toda vez que solamente pretende tipificar la acción de quien, de forma ilegítima y a través de algún medio técnico, se apodera (tiene conocimiento) de datos informáticos que son transferidos en el marco de alguna comunicación, ya sea alámbrica o inalámbrica.

Según los fundamentos del Convenio[247], esta disposición tiene como finalidad proteger el derecho a la privacidad de las comunicaciones de datos. La interceptación por "medios técnicos" se refiere a escuchar, monitorear o vigilar el contenido de las comunicaciones, a adquirir los contenidos de datos, ya sea en forma directa, mediante el acceso y uso del sistema informático, o en forma indirecta, mediante el uso de dispositivos electrónicos para escuchar en forma secreta o de dispositivos para intervenir conversaciones. La interceptación puede implicar también la grabación. El término "medios técnicos" incluye los dispositivos técnicos conectados a las líneas de transmisión, así como también los dispositivos utilizados para obtener y grabar las comunicaciones inalámbricas. Pueden incluir el uso de software, contraseñas y códigos. El requisito de que se utilice un medio técnico es una matización restrictiva destinada a evitar que se establezcan demasiados delitos.

Las comunicaciones efectuadas por los empleados, ya sean o no con fines comerciales, que constituyen "transmisiones no públicas de datos informáticos" también están protegidas contra la interceptación sin permiso[248]. La comunicación en la forma de transmisión de datos informáticos puede tener lugar dentro de un único sistema informático (por ej., pasando del CPU a la pantalla o la impresora), entre dos sistemas informáticos que pertenecen a una misma persona, entre dos ordenadores que se comunican entre sí, o entre un ordenador y una persona (por ej., a través del teclado). De acuerdo al Convenio, las Partes podrán exigir como elemento adicional que la comunicación sea transmitida entre sistemas informáticos que estén conectados de forma remota.

En la práctica, este tipo de delitos puede configurarse con los ataques de "sniffing" o ataque de interceptación. En el contexto de la seguridad de la red,

[247] Consejo de Europa, STE núm. 185, Informe Explicativo - CONVENIO SOBRE LA CIBERDELINCUENCIA; Disponible en Url: https://rm.coe.int/16802fa403

[248] Sentencia de la Corte Europea de Derechos Humanos en el caso Halford contra el Reino Unido, del 25 de junio de 1997, 20.605/92

corresponde a la interceptación de datos mediante la captura del tráfico de la red utilizando un sniffer de paquetes (una aplicación destinada a capturar paquetes de red) y su posterior análisis. La acción legítima podría estar realizada por el propietario de una red, que a fin de identificar el exceso de tráfico circulante, se dispone a capturar su propio tráfico y hacer un análisis al respecto.

Entendemos que el bien jurídico afectado no es otro que la confidencialidad de la información, ya que en definitiva, el perfeccionamiento del delito se realiza en el momento de la captura de dichos datos (por ejemplo, de una comunicación). Esta conducta, sería plenamente aplicable a los casos de escuchas ilegales, donde en definitiva, lo que está sucediendo es que el delincuente, sin estar autorizado legalmente (por los titulares de dicha comunicación o por un juez competente), interviene y registra una comunicación privada entre terceros.

Es interesante analizar si el delito efectivamente se configura para los casos donde las comunicaciones obtenidas se encuentren cifradas (por ejemplo, si realizo una captura de paquetes de una red de wifi, donde están circulando comunicaciones de la aplicación Whatsapp, que al momento de redactar estas líneas, posee un tipo de cifrado de extremo a extremo[249]). En estos casos ¿Podríamos confirmar que existe una verdadera afectación al bien jurídico afectado (confidencialidad)? Si bien la captura ilegítima efectivamente ha sucedido, lo cierto es que por la medida de seguridad implementada, dichos datos son inaccesibles (entendiendo que al día de hoy, no es conocida una técnica que permita "romper" el cifrado de dicha comunicación).

Por último, aportar que consideramos que es una figura delictiva intermedia, toda vez que, una vez que el delincuente ha ingresado y tiene posibilidad de capturar los paquetes de datos para llevar adelante la interceptación, también sería posible que realice alguna acción adicional que permitiría desviar, manipular, corromper la misma. En el caso que ello sucediera, como podría suceder con el caso de un ataque conocido en el rubro de la seguridad como "Man In The Middle" (MITM), entendemos que esta figura penal quedaría desplazada por el delito de daño informático (tratado más adelante).

---

[249] Facebook Inc; Whatsapp: https://faq.whatsapp.com/general/security-and-privacy/end-to-end- encryption/?lang=es_pe

Algunos países han considerado como un agravante el hecho de quien, imponiéndose de la comunicación a través de su interceptación ilegítima, la diere a conocer a terceros a través de su divulgación.

País	Delito 2: Interceptación ilegítima
Argentina	**CP Artículo 153:** Será reprimido con prisión de quince (15) días a seis (6) meses ... En la misma pena incurrirá el que indebidamente interceptare o captare comunicaciones electrónicas o telecomunicaciones provenientes de cualquier sistema de carácter privado o de acceso restringido. La pena será de prisión de un (1) mes a un (1) año, si el autor además comunicare a otro o publicare el contenido de la carta, escrito, despacho o comunicación electrónica. Si el hecho lo cometiere un funcionario público que abusare de sus funciones, sufrirá además, inhabilitación especial por el doble del tiempo de la condena.
Brasil	**Código Brasilero de Telecomunicações (CBT). Art. 56.** Pratica crime de violação de telecomunicação quem, transgredindo lei ou regulamento, exiba autógrafo ou qualquer documento do arquivo, divulgue ou comunique, informe ou capte, transmita a outrem ou utilize o conteúdo, resumo, significado, interpretação, indicação ou efeito de qualquer comunicação dirigida a terceiro.§ 1º Pratica, também, crime de violação de telecomunicações quem ilegalmente receber, divulgar ou utilizar, telecomunicação interceptada.§ 2º Sòmente os serviços fiscais das estações e postos oficiais poderão interceptar telecomunicação.I - A recepção de telecomunicação dirigida por quem diretamente ou como cooperação esteja legalmente autorizado;II - O conhecimento dado:a) ao destinatário da telecomunicação ou a seu representante legal;b) aos intervenientes necessários ao curso da telecomunicação;c) ao comandante ou chefe, sob cujas ordens imediatas estiver servindo;d) aos fiscais do Govêrno junto aos concessionários ou permissionários;e) ao juiz competente, mediante requisição ou intimação dêste.Parágrafo único. Não estão compreendidas nas proibições contidas nesta lei as radiocomunicações destinadas a ser livremente recebidas, as de amadores, as relativas a navios e aeronaves em perigo, ou as transmitidas nos casos de calamidade pública **LEI Nº 9.296, DE 24 DE JULHO DE 1996. Art. 10.** Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, promover escuta ambiental ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei: Pena - reclusão, de 2 (dois) a 4 (quatro) anos, e multa. (Redação dada pela Lei nº 13.869. de 2019) § 3o Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim

País	Delito 2: Interceptación ilegítima
	definidas em lei, ou o controle remoto não autorizado do dispositivo invadido: Pena – reclusão, de 2 (dois) a 5 (cinco) anos, e multa.
Colombia	**CP. Art. 269 C. Interceptación de datos informáticos.** El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.
México	**CP. Art. 168 bis:** Se impondrán de seis meses a dos años de prisión y de trescientos a tres mil días multa, a quien sin derecho: I. Descifre o decodifique señales de telecomunicaciones distintas a las de satélite portadoras de programas; II. Transmita la propiedad, uso o goce de aparatos, instrumentos o información que permitan descifrar o decodificar señales de telecomunicaciones distintas a las de satélite portadoras de programas, o III.Reciba o distribuya una señal de satélite cifrada portadora de programas originalmente codificada, sin la autorización del distribuidor legal de la señal.
España	**CP. Art. 197 2do párrafo.** El que mediante la utilización de artificios o instrumentos técnicos, y sin estar debidamente autorizado, intercepte transmisiones no públicas de datos informáticos que se produzcan desde, hacia o dentro de un sistema de información, incluidas las emisiones electromagnéticas de los mismos, será castigado con una pena de prisión de tres meses a dos años o multa de tres a doce meses

Tabla Nº 5: Cuadro comparativo de tipificación de Delito 2: Interceptación ilícita de datos

4.6.5. Delito 3: Atentado contra la integridad de los datos (cracking o daño informático)

Propuesto como obligatorio en la Convención de Cibercrimen de Budapest en el artículo 4[250] de la Sección 1. Derecho penal material - Título 1: Infracciones contra

[250] Artículo 1: "Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de actos que dañen, borren, deterioren, alteren o supriman datos informáticos. 2. Cualquier Parte podrá reservarse el derecho a exigir que los actos definidos en el apartado 1 provoquen daños graves."

la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos.

La conducta básica refiere a dañar, borrar, deteriorar, alterar o suprimir dolosamente y sin autorización datos informáticos. Alternativamente se establecen como elementos del tipo penal la necesidad de que el daño sea grave.

No existe un criterio unificado acerca de cómo realizar una tasación del daño producido para poder ser categorizado como "grave", aunque en algunos ordenamientos se considera que esa gravedad radica en afectar información sensible, confidencial, o perteneciente a sistemas pertenecientes a servicios públicos o infraestructuras consideradas como críticas.

De acuerdo a las propias explicaciones del informe explicativo del Convenio de Budapest[251], en el párrafo 1, los términos que "dañe" y "deteriore" como actos imbricados se refieren en particular a una alteración negativa de la integridad o del contenido de la información de los datos y programas. El "borrar" datos es el equivalente de la destrucción de un objeto corpóreo. Los destruye y los hace irreconocibles. Por "supresión" de datos informáticos se entiende cualquier acción que impida o ponga fin a la disponibilidad de los datos para la persona que tiene acceso al ordenador o al soporte de datos en que fueron almacenados. El término "alteración" se refiere a la modificación de los datos existentes. Por consiguiente, la introducción de códigos maliciosos, tales como virus y caballos de Troya, está incluido en este párrafo, tal como también lo está la modificación resultante de los datos.

Más allá de lo desarrollado en el Capítulo 2 de esta tesis, consideramos de importancia resaltar que esta figura penal busca proteger en la mayoría de los casos, la integridad de los datos. Sostenemos ello, toda vez que en todos los casos salvo el de supresión, el único bien jurídico afectado es la integridad de la información (remitimos a su explicación en el punto 2.2). Solamente ante el caso de supresión quedaría también afectada la disponibilidad (toda vez que deja de existir el dato, y por lo tanto, se torna indisponible para su titular). Otra excepción donde podríamos extender el bien jurídico afectado, sería dado por el caso de piezas de

[251] Consejo de Europa, STE núm. 185, Informe Explicativo - CONVENIO SOBRE LA CIBERDELINCUENCIA; Disponible en Url: https://rm.coe.int/16802fa403

malware (como Ransomware), donde la información sea ilegítimamente modificada y cifrada. En estos casos, también existiría una afectación tanto al bien jurídico de la integridad así como de la disponibilidad de los datos.

Como ya hemos visto en el delito de acceso indebido, queda pendiente el análisis de hechos donde una persona realiza una modificación o alteración ilegítima a un sistema o dato informático "pero", dicha modificación en vez de perjudicar el sistema o "dañarlo", genera una mejora en el mismo. El caso de ejemplo podría ser un sitio web, que por la mala configuración técnica que ha realizado su administrador, ha dejado puertos y vulnerabilidades expuestas que permiten que terceros accedan irrestrictamente a información confidencial (supongamos, una clínica que como está muy de moda actualmente, permite que los pacientes accedan a los resultados de sus exámenes médicos a través de un sitio web).

En el caso de ejemplo, el hacker que ingresa y modifica ilegítimamente el sitio web, lo está mejorando, implementando medidas de seguridad de las que carecía originalmente el mismo. Sin embargo, desde el punto de vista penal, podría probarse la existencia de todos los elementos del tipo penal, y rigurosamente, existió una modificación o alteración de algún dato (al menos, un 1 por un 0). Cabría preguntarnos entonces ¿Existe entonces daño informático? Entendemos que este tipo de casos podrían salvarse cuando se exige el nivel de "gravedad" que el Convenio de Budapest sugiere como elemento auxiliar, requiriendo para el momento de la imputación, la efectiva prueba de la gravedad de dicha modificación, algo que en el caso de ejemplo no parece existir.

País	Delito 3: Atentado contra la integridad de los datos
Argentina	**Art. 183 2do párrafo:** En la misma pena incurrirá el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños.

País	Delito 3: Atentado contra la integridad de los datos
Brasil	**CP. Art. 154-A.** Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita: Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa. Aumenta-se a pena de 1/3 (um terço) a 2/3 (dois terços) se da invasão resulta prejuízo econômico. § 3o Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido: Pena – reclusão, de 2 (dois) a 5 (cinco) anos, e multa.
Colombia	**CP Art. 269 D. Daño Informático.** El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.
México	**CP Artículo 211 bis 2** Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa. Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa. A quien sin autorización conozca, obtenga, copie o utilice información contenida en cualquier sistema, equipo o medio de almacenamiento informáticos de seguridad pública, protegido por algún medio de seguridad, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, destitución e inhabilitación de cuatro a diez años para desempeñarse en otro empleo, puesto, cargo o comisión pública. Las sanciones anteriores se duplicarán cuando la conducta obstruya, entorpezca, obstaculice, limite o imposibilite la procuración o impartición de justicia, o recaiga sobre los registros relacionados con un procedimiento penal resguardados por las autoridades competentes.

País	Delito 3: Atentado contra la integridad de los datos
España	**CP. Artículo 264:** 1. El que por cualquier medio, sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese o hiciese inaccesibles datos informáticos, programas informáticos o documentos electrónicos ajenos, cuando el resultado producido fuera grave, será castigado con la pena de prisión de seis meses a tres años. 2. Se impondrá una pena de prisión de dos a cinco años y multa del tanto al décuplo del perjuicio ocasionado, cuando en las conductas descritas concurra alguna de las siguientes circunstancias: 1.ª Se hubiese cometido en el marco de una organización criminal. 2.ª Haya ocasionado daños de especial gravedad o afectado a un número elevado de sistemas informáticos. 3.ª El hecho hubiera perjudicado gravemente el funcionamiento de servicios públicos esenciales o la provisión de bienes de primera necesidad. 4.ª Los hechos hayan afectado al sistema informático de una infraestructura crítica o se hubiera creado una situación de peligro grave para la seguridad del Estado, de la Unión Europea o de un Estado Miembro de la Unión Europea. A estos efectos se considerará infraestructura crítica un elemento, sistema o parte de este que sea esencial para el mantenimiento de funciones vitales de la sociedad, la salud, la seguridad, la protección y el bienestar económico y social de la población cuya perturbación o destrucción tendría un impacto significativo al no poder mantener sus funciones. 5.ª El delito se haya cometido utilizando alguno de los medios a que se refiere el artículo 264 ter. Si los hechos hubieran resultado de extrema gravedad, podrá imponerse la pena superior en grado. 3. Las penas previstas en los apartados anteriores se impondrán, en sus respectivos casos, en su mitad superior, cuando los hechos se hubieran cometido mediante la utilización ilícita de datos personales de otra persona para facilitarse el acceso al sistema informático o para ganarse la confianza de un tercero.

Tabla Nº 6: Cuadro comparativo de tipificación de Delito 3: Atentado contra la integridad de los datos

4.6.6. Delito 4: Atentados contra la integridad del sistema (Denegación de servicios)

Propuesto como obligatorio en la Convención de Cibercrimen de Budapest en el artículo 5[252] de la Sección 1. Derecho penal material - Título 1: Infracciones contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos.

La conducta básica refiere a la obstaculización o interrupción, cometida de forma dolosa y sin autorización, del funcionamiento de un sistema informático, mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos.

Dicha obstaculización no debe ser de cualquier tipo, sino que obligatoriamente debe ser considerada como grave, deliberada e ilegítima. De acuerdo al informe explicativo del Convenio de Budapest[253], cada Parte deberá determinar para sí los criterios que deberán cumplirse para que la obstaculización sea considerada "grave". Por ejemplo, una Parte puede exigir que se haya causado un mínimo de daños para que la obstaculización sea considerada grave.

Los encargados de redactar el Convenio consideraron como "grave" el envío de datos a un sistema en particular cuando su forma, tamaño o frecuencia produzca un efecto perjudicial significativo en la capacidad que tiene el dueño o el operador para utilizar dicho sistema, o para comunicarse con otros sistemas (por ej., por medio de programas que generen ataques de "denegación del servicio", códigos maliciosos como los virus que impiden o hacen considerablemente más lento el funcionamiento del sistema, o programas que envían enormes cantidades de correo

[252] "Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático mediante la introducción, transmisión, provocación de daños, borrado, deterioro, alteración o supresión de datos informáticos."

[253] Consejo de Europa, STE núm. 185, Informe Explicativo - CONVENIO SOBRE LA CIBERDELINCUENCIA; Disponible en Url: https://rm.coe.int/16802fa403

electrónico a un destinatario con el fin de bloquear las funciones de comunicación del sistema).

Adicionalmente, la obstaculización debe ser "ilegítima". Las actividades comunes inherentes al diseño de las redes, o las prácticas comerciales y de operación comunes, se efectúan de manera legítima. Las mismas incluyen, por ej., la verificación de la seguridad de un sistema informático, o su protección, autorizada por su propietario o por el operador, o la reconfiguración del sistema operativo de un ordenador que tiene lugar cuando el operador de un sistema instala un nuevo software que inhabilita programas similares previamente instalados. Por lo tanto, dicha conducta no constituye un delito conforme a este artículo, incluso si causa una obstaculización seria.

País	Delito 4: Atentado contra la Integridad del sistema
Argentina	**CP Art. 183 2do párrafo:** En la misma pena incurrirá el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños. **CP Artículo 197:** Será reprimido con prisión de seis (6) meses a dos (2) años, el que interrumpiere o entorpeciere la comunicación telegráfica, telefónica o de otra naturaleza o resistiere violentamente el restablecimiento de la comunicación interrumpida.
Brasil	**CP. Art. 266:** Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública: Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento: Pena - detenção, de um a três anos, e multa. § 1o Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento. (Incluído pela Lei nº 12.737, de 2012) Vigência § 2o Aplicam-se as penas em dobro se o crime é cometido por ocasião de calamidade pública. (Incluído pela Lei nº 12.737, de 2012) Vigência

País	Delito 4: Atentado contra la Integridad del sistema
Colombia	**CP Art. 269 B:** Obstaculización ilegítima de sistema informático o red de telecomunicación. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

País	Delito 4: Atentado contra la Integridad del sistema
México	**CP Artículo 211 bis 2:** Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa. Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa. A quien sin autorización conozca, obtenga, copie o utilice información contenida en cualquier sistema, equipo o medio de almacenamiento informáticos de seguridad pública, protegido por algún medio de seguridad, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, destitución e inhabilitación de cuatro a diez años para desempeñarse en otro empleo, puesto, cargo o comisión pública. Las sanciones anteriores se duplicarán cuando la conducta obstruya, entorpezca, obstaculice, limite o imposibilite la procuración o impartición de justicia, o recaiga sobre los registros relacionados con un procedimiento penal resguardados por las autoridades competentes. **Artículo 211 bis 3** Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de dos a ocho años de prisión y de trescientos a novecientos días multa. Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente copie información que contengan, se le impondrán de uno a cuatro años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa. A quien estando autorizado para acceder a sistemas, equipos o medios de almacenamiento informáticos en materia de seguridad pública, indebidamente obtenga, copie o utilice información que contengan, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, hasta una mitad más de la pena impuesta, destitución e inhabilitación por un plazo igual al de la pena resultante para desempeñarse en otro empleo, puesto, cargo o comisión pública. **Artículo 211 bis 4** Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a cuatro

País	Delito 4: Atentado contra la Integridad del sistema
	años de prisión y de cien a seiscientos días multa. Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa. **Artículo 211 bis 5** Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa. Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente copie información que contengan, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa. Las penas previstas en este artículo se incrementarán en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero
España	**CP. Artículo 264 bis.** 1. Será castigado con la pena de prisión de seis meses a tres años el que, sin estar autorizado y de manera grave, obstaculizara o interrumpiera el funcionamiento de un sistema informático ajeno: a) realizando alguna de las conductas a que se refiere el artículo anterior; b) introduciendo o transmitiendo datos; o c) destruyendo, dañando, inutilizando, eliminando o sustituyendo un sistema informático, telemático o de almacenamiento de información electrónica. Si los hechos hubieran perjudicado de forma relevante la actividad normal de una empresa, negocio o de una Administración pública, se impondrá la pena en su mitad superior, pudiéndose alcanzar la pena superior en grado. 2. Se impondrá una pena de prisión de tres a ocho años y multa del triplo al décuplo del perjuicio ocasionado, cuando en los hechos a que se refiere el apartado anterior hubiera concurrido alguna de las circunstancias del apartado 2 del artículo anterior. 3. Las penas previstas en los apartados anteriores se impondrán, en sus respectivos casos, en su mitad superior, cuando los hechos se hubieran cometido mediante la utilización ilícita de datos personales de otra persona para facilitarse el acceso al sistema informático o para ganarse la confianza de un tercero.

Tabla Nº 7: Cuadro comparativo de tipificación de Delito 3: Atentado contra la integridad del sistema.

4.6.7. Delito 5: Abuso de Dispositivos

Propuesto como obligatorio en la Convención de Cibercrimen de Budapest en el artículo 6[254] de la Sección 1. Derecho penal material - Título 1: Infracciones contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos.

La conducta básica planteada en el punto 1 refiere a la producción, venta, obtención para su utilización, importación, difusión u otras formas de puesta a disposición de un dispositivo, incluido un programa informático, principalmente concebido o adaptado para permitir la comisión de otros delitos. En esta parte, podríamos considerar incluída la producción y difusión de malware, que como ya veremos es considerada por muchas normativas como parte del delito de daño informático antes analizada.

También propone la consideración como delito la venta, obtención para su utilización y difusión (ilegítima) de las credenciales (usuario y contraseña) que permitan acceder a todo o parte de un sistema informático, con la intención de utilizarlos como medio para cometer otros delitos. Esta propuesta es de sumo interés toda vez que a nivel estadístico[255] el *phishing* (entendido por este autor como la

---

[254] Art. 6: "1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de los siguientes actos: a) La producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de: i) Un dispositivo, incluido un programa informático, diseñado o adaptado principalmente para la comisión de cualquiera de los delitos previstos de conformidad con los anteriores artículos 2 a 5; ii) Una contraseña, un código de acceso o datos informáticos similares que permitan tener acceso a la totalidad o a una parte de un sistema informático, con el fin de que sean utilizados para la comisión de cualquiera de los delitos contemplados en los artículos 2 a 5; y b) la posesión de alguno de los elementos contemplados en los anteriores apartados a.i) o ii) con el fin de que sean utilizados para cometer cualquiera de los delitos previstos en los artículos 2 a 5. Cualquier Parte podrá exigir en su derecho interno que se posea un número determinado de dichos elementos para que se considere que existe responsabilidad penal.

2. No podrá interpretarse que el presente artículo impone responsabilidad penal en los casos en que la producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición mencionadas en el apartado 1 del presente artículo no tengan por objeto la comisión de un delito previsto de conformidad con los artículos 2 a 5 del presente Convenio, como es el caso de las pruebas autorizadas o de la protección de un sistema informático. 3. Cualquier Parte podrá reservarse el derecho a no aplicar lo dispuesto en el apartado 1 del presente artículo, siempre que la reserva no afecte a la venta, la distribución o cualquier otra puesta a disposición de los elementos indicados en el apartado 1.a.ii) del presente artículo.

[255] WeLiveSecurity; "Los ataques de phishing apuntando a usuarios de redes sociales pasó de 11.8% en el último cuarto de 2020 a 23.6% durante los primeros tres meses de 2021, con cibercriminales lanzando ataques con el objetivo de secuestrar cuentas de redes sociales para probablemente comercializar los accesos en mercados de la dark web.", Url: https://www.welivesecurity.com/la-es/2021/06/15/2021-registro-pico-historico-cantidad-sitios-phishing/

captación ilegítimas de datos confidenciales, en su mayoría, credenciales de acceso) es una de las figuras de mayor crecimiento en el mundo del cibercrimen. Dejaremos el análisis de este fenómenos para los capítulos finales de este trabajo, donde podremos ver con mayor claridad, la dimensión y las consecuencias del crecimiento de esta actividad.

Alternativamente el Convenio propone también la tipificación penal de la mera tenencia (tenencia simple) de los elementos descritos -dispositivo, programa informático, códigos de acceso- aunque existen diferencias de criterios al respecto sobre su viabilidad técnica-jurídica, en el sentido que consiste en un adelantamiento cada vez más lejano de la barrera penal.

Entre los fundamentos expresados por la Comisión[256] al momento de su redacción se sostiene que estos delitos a menudo requiere la posesión de medios de acceso ("herramientas de piratería") o de otras herramientas, y como existe un fuerte incentivo para adquirirlas con fines delictivos, lo que puede luego llevar a la creación de una especie de mercado negro para su producción y distribución. Con el fin de combatir dichos peligros con mayor eficacia, el derecho penal debería prohibir en su origen los actos específicos que sean potencialmente peligrosos, antes de que se cometan los delitos previstos en los Artículos 2 a 5. En lo que a esto se refiere, esta disposición se basa en desarrollos recientes en el seno del Consejo de Europa (Convenio Europeo sobre la protección jurídica de los servicios de acceso condicional o basados en dicho acceso – STE núm. 178) y de la Unión Europea (Directiva 98/84/CE del Parlamento Europeo y del Consejo, de 20 de noviembre de 1998, relativa a la protección jurídica de los servicios de acceso condicional o basados en dicho acceso) y las disposiciones pertinentes en algunos países. Un enfoque similar había sido ya adoptado en el Convenio internacional sobre represión de la falsificación de moneda firmado en Ginebra en 1929.

Consideramos super valioso e importante la incorporación, en el párrafo tercero, de una eximición manifiesta de responsabilidad penal para los casos donde la producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición mencionadas en el apartado 1 del presente artículo no

[256] Consejo de Europa, STE núm. 185, Informe Explicativo - CONVENIO SOBRE LA CIBERDELINCUENCIA; Disponible en Url: https://rm.coe.int/16802fa403

tengan por objeto la comisión de un delito previsto de conformidad con los artículos 2 a 5 del presente Convenio, como es el caso de las pruebas autorizadas o de la protección de un sistema informático.

Es importante la visibilización de estas posibilidades a nivel jurídico, toda vez que en el mundo de la investigación de la seguridad de la información, a fin de comprender el funcionamiento de estos sistemas (y sus vulnerabilidades), es necesario contar con este tipo de equipos y programas informáticos. Si bien, como dice el maestro Riquert[257], puede ser redundante por no existir en esos casos la intención de cometer algunas de las infracciones enumeradas, no menos cierto es que la prueba de dichas intenciones, en el marco del proceso penal, se hace muchas veces complicada para el investigador (frente a una fiscalía convencida de lo contrario).

La existencia de casos con injusticias claras al respecto se encuentra el paradigmático caso de Ola Bini[258], desarrollador de software sueco que reside en Ecuador desde el 2013, quien a pesar de ser considerado por muchos como uno de los mejores programadores y expertos en seguridad digital en el mundo, y haber mejorado la seguridad y privacidad de usuarios de internet a través de su trabajo, fue arrestado por autoridades ecuatorianas en abril del 2019, sin existir acusaciones formales en su contra en el momento del arresto ni pruebas de haber quebrantado alguna ley que lo vincularse a algún delito.

Este tipo de casos ha despertado el interés de asociaciones internacionales como Access Now[259], quien ha lanzado un elaborado y publicado el mes de agosto del 2021, titulado “La persecución de la comunidad de la seguridad informática en América Latina”. Dicho informe detalla las leyes vigentes sobre ciberseguridad en países latinoamericanos, como Argentina, Colombia, Ecuador y México; además,

---

[257] RIQUERT, Marcelo Alfredo. “Algo más sobre la Legislación contra la Delincuencia Informática en MERCOSUR a propósito de la Modificación al Código Penal Argentino por Ley 26388”, publicado en AR-DI, Nº 121, Agosto 2008.

[258] CNN, “Comienza el juicio de Ola Bini, amigo de Julian Assange, acusado por presunto acceso ilegal a sistema informático en Ecuador”, Url: https://cnnespanol.cnn.com/2022/01/19/el-juicio-de-ola-bini-amigo-de-julian-assange-en-ecuador-orix/

[259] Access Now, es una organización sin fines de lucro a escala mundial, apunta a crear conciencia sobre el trato perjudicial de los gobiernos en relación con los investigadores de seguridad digital, tanto en la ley como en la práctica.

analiza casos emblemáticos de acoso, persecución y criminalización a investigadores de seguridad digital en dichos países.

Dicho informe, realiza el tratamiento de distintos casos, entre ellos, uno de conocimiento público en Argentina, de persecución al desarrollador informático Javier Smaldone, quien fue sistemáticamente perseguido, allanado y procesado, sin existir pruebas concretas en su contra (Javier fue sobreseído después de muchos años).

País	Delito 5: Abuso de los dispositivos
Argentina	**Parcialmente aplicable. CP Art. 183 2do párrafo:** En la misma pena incurrirá el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños.
Brasil	
Colombia	**Parcialmente aplicable. CP Artículo 269E. Uso de software malicioso.** El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes. **CP Artículo 269F: Violación de datos personales.** El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes. **CP Artículo 269G: Suplantación de sitios web para capturar datos personales.**

País	Delito 5: Abuso de los dispositivos
	El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave. En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave. La pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito.
México	**Parcialmente aplicable. CP. Art. 168 ter.** Se sancionará con pena de doce a quince años de prisión, a quien fabrique, comercialice, adquiera, instale, porte, use u opere equipos que bloqueen, cancelen o anulen las señales de telefonía celular, de radiocomunicación o de transmisión de datos o imagen con excepción de lo establecido en el segundo párrafo del artículo 190 Bis de la Ley Federal de Telecomunicaciones y Radiodifusión. Los equipos a que hace referencia el primer párrafo del artículo 190 Bis de la Ley Federal de Telecomunicaciones y Radiodifusión, serán asegurados en términos de lo que establece el Código Nacional de Procedimientos Penales y posteriormente deberán ser destruidos en su totalidad. Si el delito al que se refiere el primer párrafo de este artículo, fuera cometido por servidores públicos, y sin autorización expresa escrita debidamente acreditada por su superior inmediato, se le impondrá la pena de quince a dieciocho años de prisión. **Parcialmente aplicable. CP Art. 424 bis.-** Se impondrá prisión de tres a diez años y de dos mil a veinte mil días multa: I. A quien produzca, reproduzca, introduzca al país, almacene, transporte, distribuya, venda o arriende copias de obras, fonogramas, videogramas o libros, protegidos por la Ley Federal del Derecho de Autor, en forma dolosa, con fin de especulación comercial y sin la autorización que en los términos de la citada Ley deba otorgar el titular de los derechos de autor o de los derechos conexos. Igual pena se impondrá a quienes, a sabiendas, aporten o provean de cualquier forma, materias primas o insumos destinados a la producción o reproducción de obras, fonogramas, videogramas o libros a que se refiere el párrafo anterior; Párrafo reformado DOF 01-07-2020 II. A quien fabrique con fin de lucro un dispositivo o sistema cuya finalidad sea desactivar los dispositivos electrónicos de protección de un programa de computación, o Fracción reformada DOF 01-07-2020

País	Delito 5: Abuso de los dispositivos
	III.A quien grabe, transmita o realice una copia total o parcial de una obra cinematográfica protegida, exhibida en una sala de cine o lugares que hagan sus veces, sin la autorización del titular del derecho de autor o derechos conexos.
España	CP Artículo 197 ter. Será castigado con una pena de prisión de seis meses a dos años o multa de tres a dieciocho meses el que, sin estar debidamente autorizado, produzca, adquiera para su uso, importe o, de cualquier modo, facilite a terceros, con la intención de facilitar la comisión de alguno de los delitos a que se refieren los apartados 1 y 2 del artículo 197 o el artículo 197 bis: a) un programa informático, concebido o adaptado principalmente para cometer dichos delitos; o b) una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información.

Tabla Nº 8: Cuadro comparativo de tipificación de Delito 5: Abuso de Dispositivos

4.6.8. Delito 6: Falsedad Informática

Propuesto como obligatorio en la Convención de Cibercrimen de Budapest en el artículo 7[260] de la Sección 1. Derecho penal material - Título 2: Infracciones informáticas, la conducta básica refiere a la introducción, alteración, borrado o supresión dolosa y sin autorización de datos informáticos, generando datos no auténticos, con la intención de que sean percibidos o utilizados a efectos legales como auténticos, con independencia de que sean directamente legibles e inteligibles.

Alternativamente se establecen como elementos del tipo penal la exigencia de ánimo fraudulento o de cualquier otro ánimo similar para que nazca responsabilidad penal.

[260] Artículo 7. Falsificación informática: "Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno, cuando se cometa de forma deliberada e ilegítima, la introducción, alteración, borrado o supresión de datos informáticos que dé lugar a datos no auténticos, con la intención de que sean tenidos en cuenta o utilizados a efectos legales como si se tratara de datos auténticos, con independencia de que los datos sean o no directamente legibles e inteligibles. Cualquier Parte podrá exigir que exista una intención fraudulenta o una intención delictiva similar para que se considere que existe responsabilidad penal."

Esta figura se nos presenta como un caso especial de daño informático (por lo que, en el caso de regularse, debería tener penas más altas que otras figuras básicas), toda vez que en su interior existe un caso de modificación o alteración ilegítima, pero con la característica puntual que aquí, se pretende que dichas modificaciones luzcan como "auténticas" frente al legítimo titular.

Por un lado, esta figura bien tipificada podría ser de utilidad para la persecución de los casos de phishing, entendiendo que la modalidad básica consiste en la generación de un sitio falso (que en apariencia, parece verdadero frente al usuario) de entidades bancarias, servicios de correo electrónico, etc.

Como se afirma en los fundamentos de su redacción[261], la finalidad de este artículo es establecer un delito paralelo al de falsificación de documentos tangibles. Su objetivo es colmar algunas lagunas en el derecho penal en relación con el delito de falsificación tradicional, que requiere la legibilidad visual de las afirmaciones o declaraciones contenidas en un documento y que no se aplica a los datos almacenados electrónicamente.

Las manipulaciones de dichos datos con valor probatorio pueden tener las mismas consecuencias graves que los actos de falsificación tradicionales si un tercero se ve así engañado. La falsificación informática implica la creación o la alteración ilegítimas de los datos almacenados de manera tal que adquieran un valor probatorio diferente en el transcurso de transacciones legales, que se basan en la autenticidad de la información contenida en los datos, y es objeto de un engaño. El interés jurídico que se desea proteger es la seguridad y la fiabilidad de los datos electrónicos, que pueden tener consecuencias para las relaciones legales.

Según sus redactores, esta disposición abarca datos que sean equivalentes a un documento de carácter público o privado, que tenga efectos legales. La "introducción" no autorizada de datos correctos o incorrectos produce una situación que se corresponde con la elaboración de un documento falso. Las posteriores alteraciones (modificaciones, variaciones, cambios parciales), borrado (eliminación de datos de un soporte de datos) y supresiones (retención, ocultación de datos) corresponden en general al delito de falsificación de un documento auténtico.

[261] Consejo de Europa, STE núm. 185, Informe Explicativo - CONVENIO SOBRE LA CIBERDELINCUENCIA; Disponible en Url: https://rm.coe.int/16802fa403

Con este sentido, esta figura podría ser aplicable por ejemplo a la creación de cheques o comprobantes de pago falsos (algo muy común en algunas modalidades de estafa), que pretenden lucir como verdaderos ante las víctimas, para que estas últimas hagan o dejen de realizar alguna acción determinada.

País	Delito 6: Falsedad Informática
Argentina	**Ley Nº 26.388: Art. 77** "...El término documento comprende toda representación de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión. Los términos firma y suscripción comprenden la firma digital, la creación de una firma digital o firmar digitalmente. Los términos instrumento privado y certificado comprenden el documento digital firmado digitalmente **Parcialmente aplicable. ARTICULO 292.-** El que hiciere en todo o en parte un documento falso o adultere uno verdadero, de modo que pueda resultar perjuicio, será reprimido con reclusión o prisión de uno a seis años, si se tratare de un instrumento público y con prisión de seis meses a dos años, si se tratare de un instrumento privado. Si el documento falsificado o adulterado fuere de los destinados a acreditar la identidad de las personas o la titularidad del dominio o habilitación para circular de vehículos automotores, la pena será de tres a ocho años. **Parcialmente aplicable. ARTÍCULO 183 2do párrafo:** En la misma pena incurrirá el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños.
Brasil	**Parcialmente aplicable. CP 298. Falsificação de documento particular** Art. 298 - Falsificar, no todo ou em parte, documento particular ou alterar documento particular verdadeiro: Pena - reclusão, de um a cinco anos, e multa. **Falsificação de cartão** Parágrafo único. Para fins do disposto no caput, equipara-se a documento particular o cartão de crédito ou débito.
Colombia	**Parcialmente aplicable. Artículo 269D: Daño Informático.** El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

País	Delito 6: Falsedad Informática
	Parcialmente aplicable. Artículo 269G: Suplantación de sitios web para capturar datos personales. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave. En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave. La pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito.
México	**Parcialmente aplicable. Artículo 211 bis 3.-** Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de dos a ocho años de prisión y de trescientos a novecientos días multa. Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente copie información que contengan, se le impondrán de uno a cuatro años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa. A quien estando autorizado para acceder a sistemas, equipos o medios de almacenamiento informáticos en materia de seguridad pública, indebidamente obtenga, copie o utilice información que contengan, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, hasta una mitad más de la pena impuesta, destitución e inhabilitación por un plazo igual al de la pena resultante para desempeñarse en otro empleo, puesto, cargo o comisión pública. **Parcialmente aplicable. Artículo 211 bis 4.-** Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa. Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

País	Delito 6: Falsedad Informática
	Parcialmente aplicable. Artículo 211 bis 5.- Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa. Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente copie información que contengan, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa. Las penas previstas en este artículo se incrementarán en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero.
España	**Parcialmente aplicable.** Artículo 399 bis. 1. El que altere, copie, reproduzca o de cualquier otro modo falsifique tarjetas de crédito o débito, cheques de viaje o cualquier otro instrumento de pago distinto del efectivo, será castigado con la pena de prisión de cuatro a ocho años. Se impondrá la pena en su mitad superior cuando los efectos falsificados afecten a una generalidad de personas o cuando los hechos se cometan en el marco de una organización criminal dedicada a estas actividades. Cuando de acuerdo con lo establecido en el artículo 31 bis una persona jurídica sea responsable de los anteriores delitos, se le impondrá la pena de multa de dos a cinco años. Atendidas las reglas establecidas en el artículo 66 bis, los jueces y tribunales podrán asimismo imponer las penas recogidas en las letras b) a g) del apartado 7 del artículo 33. 2. La tenencia de tarjetas de crédito o débito, cheques de viaje o cualesquiera otros instrumentos de pago distintos del efectivo falsificados, destinados a la distribución o tráfico será castigada con la pena señalada a la falsificación. 3. El que sin haber intervenido en la falsificación usare, en perjuicio de otro y a sabiendas de la falsedad, tarjetas de crédito o débito, cheques de viaje o cualesquiera otros instrumentos de pago distintos del efectivo falsificados, será castigado con la pena de prisión de dos a cinco años. 4. El que, para su utilización fraudulenta y a sabiendas de su falsedad, posea u obtenga, para sí o para un tercero, tarjetas de crédito o débito, cheques de viaje o cualquier otro instrumento de pago distinto del efectivo será castigado con pena de prisión de uno a dos años. **Parcialmente aplicable.** Artículo 399 ter. A los efectos de este Código, se entiende por instrumento de pago distinto del efectivo cualquier dispositivo, objeto o registro protegido, material o inmaterial, o una combinación de estos, exceptuada la moneda de curso legal, que, por sí solo o en combinación con un procedimiento o conjunto de procedimientos, permite al titular o usuario transferir dinero o valor monetario incluso a través de medios digitales de intercambio.

País	Delito 6: Falsedad Informática
	Parcialmente aplicable. Artículo 249. 1. También se consideran reos de estafa y serán castigados con la pena de prisión de seis meses a tres años: a) Los que, con ánimo de lucro, obstaculizando o interfiriendo indebidamente en el funcionamiento de un sistema de información o introduciendo, alterando, borrando, transmitiendo o suprimiendo indebidamente datos informáticos o valiéndose de cualquier otra manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro. b) Los que, utilizando de forma fraudulenta tarjetas de crédito o débito, cheques de viaje o cualquier otro instrumento de pago material o inmaterial distinto del efectivo o los datos obrantes en cualquiera de ellos, realicen operaciones de cualquier clase en perjuicio de su titular o de un tercero. 2. Con la misma pena prevista en el apartado anterior serán castigados: a) Los que fabricaren, importaren, obtuvieren, poseyeren, transportaren, comerciaren o de otro modo facilitaren a terceros dispositivos, instrumentos o datos o programas informáticos, o cualquier otro medio diseñado o adaptado específicamente para la comisión de las estafas previstas en este artículo. b) Los que, para su utilización fraudulenta, sustraigan, se apropiaren o adquieran de forma ilícita tarjetas de crédito o débito, cheques de viaje o cualquier otro instrumento de pago material o inmaterial distinto del efectivo. 3. Se impondrá la pena en su mitad inferior a los que, para su utilización fraudulenta y sabiendo que fueron obtenidos ilícitamente, posean, adquieran, transfieran, distribuyan o pongan a disposición de terceros tarjetas de crédito o débito, cheques de viaje o cualesquiera otros instrumentos de pago materiales o inmateriales distintos del efectivo.

Tabla Nº 9: Cuadro comparativo de tipificación de Delito 6: Falsedad Informática

4.6.9. Delito 7: Fraude o Estafa Informática

Propuesto como obligatorio en la Convención de Cibercrimen de Budapest en el artículo 8[262] de la Sección 1. Derecho penal material - Título 2: Infracciones informáticas.

Nuevamente estamos ante casos especiales de la figura básica del cracking, toda vez que la figura requiere inicialmente cualquier introducción, alteración, borrado o supresión de datos informáticos; o cualquier interferencia en el funcionamiento de un sistema informático, con la intención fraudulenta o delictiva de obtener ilegítimamente un beneficio económico para uno mismo o para otra persona.

La finalidad de este artículo es establecer como delito toda manipulación indebida realizada en el transcurso del procesamiento de datos con la intención de efectuar una transferencia ilegal de bienes (generando un perjuicio económico en la víctima).

De acuerdo al considerando Nº 90 de los fundamentos del Convenio de Budapest, este delito debe ser cometido de manera “deliberada" (igual a los anteriores). El elemento general de la intención deliberada se refiere a la manipulación o la interferencia de los equipos informáticos que cause un perjuicio patrimonial a un tercero.

El delito requiere también la existencia de una intención deliberada específica de índole fraudulenta o dolosa para obtener un beneficio económico o de otro tipo para sí o para otra persona. Así, por ejemplo, no se pretende incluir en el delito establecido por este artículo aquellas prácticas comerciales con respecto a la competencia en el mercado, que pueden causar un perjuicio patrimonial a una persona y beneficiar a otra, pero que no son llevadas a cabo con una intención fraudulenta o dolosa.

[262] Artículo 8. Fraude informático: “Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno los actos deliberados e ilegítimos que causen un perjuicio patrimonial a otra persona mediante: a) Cualquier introducción, alteración, borrado o supresión de datos informáticos; b) cualquier interferencia en el funcionamiento de un sistema informático, con la intención fraudulenta o delictiva de obtener ilegítimamente un beneficio económico para uno mismo o para otra persona.”

Otro caso de ejemplo es qie no se pretende establecer como delito el uso de programas que reúnen información para comparar los precios de las compras que se pueden hacer por Internet ("bots"), incluso si no son autorizados por un sitio visitado por el “bot".

País	Delito 7: Fraude o Estafa Informática
Argentina	**CP Art. 173 - Inciso 16.** El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos. **CP Art. 172 CP:** Será reprimido con prisión de un mes a seis años, el que defraudare a otro con nombre supuesto, calidad simulada, falsos títulos, influencia mentida, abuso de confianza o aparentando bienes, crédito, comisión, empresa o negociación o valiéndose de cualquier otro ardid o engaño.
Brasil	**CP: Furto - Art. 155** Subtrair, para si ou para outrem, coisa alheia móvel: Pena - reclusão, de um a quatro anos, e multa. § 1º - A pena aumenta-se de um terço, se o crime é praticado durante o repouso noturno. § 2º - Se o criminoso é primário, e é de pequeno valor a coisa furtada, o juiz pode substituir a pena de reclusão pela de detenção, diminuí-la de um a dois terços, ou aplicar somente a pena de multa. § 3º - Equipara-se à coisa móvel a energia elétrica ou qualquer outra que tenha valor econômico. Furto qualificado § 4º - A pena é de reclusão de dois a oito anos, e multa, se o crime é cometido: I - com destruição ou rompimento de obstáculo à subtração da coisa; II - com abuso de confiança, ou mediante fraude, escalada ou destreza; III - com emprego de chave falsa; IV - mediante concurso de duas ou mais pessoas. § 4º-A A pena é de reclusão de 4 (quatro) a 10 (dez) anos e multa, se houver emprego de explosivo ou de artefato análogo que cause perigo comum. (Incluído pela Lei nº 13.654, de 2018) § 4º-B. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se o furto mediante fraude é cometido por meio de dispositivo eletrônico ou informático, conectado ou não à rede de computadores, com ou sem a violação de mecanismo de segurança ou a utilização de programa malicioso, ou por qualquer outro meio fraudulento análogo. (Incluído pela Lei nº 14.155, de 2021)

País	Delito 7: Fraude o Estafa Informática
Colombia	**CP Artículo 269I: Hurto por medios informáticos y semejantes.** El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 de este Código. **CP Art. 269 J: Transferencia no consentida de activos.** El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1.500 salarios mínimos legales mensuales vigentes. La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa. Si la conducta descrita en los dos incisos anteriores tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad.
México	**CP Artículo 386.** Comete el delito de fraude el que engañando a uno o aprovechándose del error en que éste se halla se hace ilícitamente de alguna cosa o alcanza un lucro indebido. El delito de fraude se castigará con las penas siguientes: I.- Con prisión de 3 días a 6 meses o de 30 a 180 días multa, cuando el valor de lo defraudado no exceda de diez veces el salario; II.- Con prisión de 6 meses a 3 años y multa de 10 a 100 veces el salario, cuando el valor de lo defraudado excediera de 10, pero no de 500 veces el salario; III.- Con prisión de tres a doce años y multa hasta de ciento veinte veces el salario, si el valor de lo defraudado fuere mayor de quinientas veces el salario.
España	**CP Artículo 248.** Cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno. Los reos de estafa serán castigados con la pena de prisión de seis meses a tres años. Para la fijación de la pena se tendrá en cuenta el importe de lo defraudado, el quebranto económico causado al perjudicado, las relaciones entre este y el defraudador, los medios empleados por este y cuantas otras circunstancias sirvan para valorar la gravedad de la infracción. Si la cuantía de lo defraudado no excediere de 400 euros, se impondrá la pena de multa de uno a tres meses. **CP Artículo 249.** 1. También se consideran reos de estafa y serán castigados con la pena de prisión de seis meses a tres años:

País	Delito 7: Fraude o Estafa Informática
	a) Los que, con ánimo de lucro, obstaculizando o interfiriendo indebidamente en el funcionamiento de un sistema de información o introduciendo, alterando, borrando, transmitiendo o suprimiendo indebidamente datos informáticos o valiéndose de cualquier otra manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro. b) Los que, utilizando de forma fraudulenta tarjetas de crédito o débito, cheques de viaje o cualquier otro instrumento de pago material o inmaterial distinto del efectivo o los datos obrantes en cualquiera de ellos, realicen operaciones de cualquier clase en perjuicio de su titular o de un tercero. 2. Con la misma pena prevista en el apartado anterior serán castigados: a) Los que fabricaren, importaren, obtuvieren, poseyeren, transportaren, comerciaren o de otro modo facilitaren a terceros dispositivos, instrumentos o datos o programas informáticos, o cualquier otro medio diseñado o adaptado específicamente para la comisión de las estafas previstas en este artículo. b) Los que, para su utilización fraudulenta, sustraigan, se apropiaren o adquieran de forma ilícita tarjetas de crédito o débito, cheques de viaje o cualquier otro instrumento de pago material o inmaterial distinto del efectivo. 3. Se impondrá la pena en su mitad inferior a los que, para su utilización fraudulenta y sabiendo que fueron obtenidos ilícitamente, posean, adquieran, transfieran, distribuyan o pongan a disposición de terceros tarjetas de crédito o débito, cheques de viaje o cualesquiera otros instrumentos de pago materiales o inmateriales distintos del efectivo.

Tabla Nº 10: Cuadro comparativo de tipificación de Delito 7: Fraude o Estafa Informática

4.6.10. Delito 8: Material de Abuso Sexual Infantil

Propuesto como obligatorio en la Convención de Cibercrimen de Budapest en el artículo 9[263] de la Sección 1. Derecho penal material - Título 3: Infracciones relativas al contenido.

La conducta básica refiere a la producción, ofrecimiento, puesta a disposición, difusión, transmisión, comercialización, de "pornografía infantil" a través de un sistema informático.

De acuerdo al Protocolo Facultativo de la Convención sobre los derechos del niño, relativo a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía[264], adoptada y abierta a la firma y ratificación, o adhesión, por la Asamblea General en su Resolución A/RES/54/263 de 25 de mayo de 2000. En el Art. 2º, inc. C de dicho instrumento se establece que "*por pornografía infantil se entiende toda representación, por cualquier medio, de un niño dedicado a actividades sexuales explícitas, reales o simuladas, o toda representación de las partes genitales de un niño con fines primordialmente sexuales*".

Además, debemos tener en consideración que actualmente entre los delitos informáticos más graves están aquellos donde el bien jurídico afectado es la integridad sexual del menor, por lo se ha optado por su inclusión de este delito de difusión o tenencia de material de abuso sexual infantil en el cuadro de delitos a

[263] Artículo 9: "1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de los siguientes actos: a) La producción de pornografía infantil con vistas a su difusión por medio de un sistema informático; b) la oferta o la puesta a disposición de pornografía infantil por medio de un sistema informático; c) la difusión o transmisión de pornografía infantil por medio de un sistema informático, d) la adquisición de pornografía infantil por medio de un sistema informático para uno mismo o para otra persona; e) la posesión de pornografía infantil en un sistema informático o en un medio de almacenamiento de datos informáticos. 2. A los efectos del anterior apartado 1, por «pornografía infantil» se entenderá todo material pornográfico que contenga la representación visual de: a) Un menor comportándose de una forma sexualmente explícita; b) una persona que parezca un menor comportándose de una forma sexualmente explícita; c) imágenes realistas que representen a un menor comportándose de una forma sexualmente explícita. 3. A los efectos del anterior apartado 2, por «menor» se entenderá toda persona menor de dieciocho años. No obstante, cualquier Parte podrá establecer un límite de edad inferior, que será como mínimo de dieciséis años. 4. Cualquier Parte podrá reservarse el derecho a no aplicar, en todo o en parte, las letras d) y e) del apartado 1, y las letras b) y c) del apartado 2."

[264] NACIONES UNIDAS, "Protocolo facultativo de la Convención sobre los Derechos del Niño relativo a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía", Url: https://www.unicef.org/spanish/specialsession/documentation/documents/op_se_sp.pdf

analizar, toda vez que consideramos de interés poder observar los distintos criterios[265] receptados en cada país en relación a este tema.

A modo de corolario, no queremos dejar de expresar que en la actualidad, y bajo una adecuada perspectiva de género, se considera inadecuado hablar de "porno infantil" o "pornografía infantil". ¿Por qué? Porque los niños fotografiados o grabados mientras están siendo víctimas de abusos sexuales merecen ser protegidos y respetados. La gravedad de su abuso no debería reducirse con el uso de palabras como "porno".

La pornografía es un término utilizado para adultos que realizan actos sexuales consentidos y distribuidos casi siempre de forma lícita al público en general para su disfrute sexual. *Si hay niños implicados, no es porno. Es un delito. Es abuso.*[266] Adherimos a que estos términos no deberían formar parte del lenguaje legítimo utilizado por los organismos encargados de la aplicación de la ley, la judicatura, el público o los medios.

Las Orientaciones terminológicas para la protección de niñas, niños y adolescentes contra la explotación y el abuso sexual, también conocidas como las Orientaciones de Luxemburgo, ofrecen una directriz clara sobre cómo guiar el complejo léxico normalmente utilizado al hablar de explotación y abusos sexuales de menores.

Las Orientaciones de Luxemburgo fueron elaboradas por un grupo de 18 socios internacionales, inclusive INTERPOL. Consideramos estas orientaciones como las mejores prácticas y recomendamos su uso a los organismos encargados de la aplicación de la ley de todo el mundo.

En el ámbito judiical, la Suprema Corte de Justicia de Mendoza recomienda en una reciente acordada (Número 29.363) no hablar más de "pornografía infantil", "Es una recomendación de la Corte al resto de los jueces. Cuando uno afirma 'pornografía infantil' y reflexiona, se da cuenta de que está hablando de una

[265] Algunos países como Argentina por ejemplo, han decidido que será considerado delito penal la tenencia con fines inequívocos de distribución o comercialización (art. 128 CP). Otros, como Chile, considera como delito penal la simple tenencia de pornografía infantil (art. 374 bis).

[266] INTERPOL, "Terminología adecuada", url: https://www.interpol.int/es/Delitos/Delitos-contra-menores/Terminologia-apropiada

actividad que es imposible que sea lícita. El tema es que la pornografía sí es una actividad lícita, pero no hay forma que cuando involucre a un niño o niña pueda ser legal", destacó el ministro de la Corte, Mario Adaro.[267]

Alternativamente se propone también la tipificación penal de la sola tenencia de pornografía infantil, existen diferencias de criterios al respecto sobre su viabilidad técnica-jurídica.

Tanto en la región de Argentina como Brasil, luego de la primera aproximación —año 2003— en la discusión parlamentaria de sus respectivas leyes modificatorias internas, se optó por excluir las meras simulaciones de los tipos penales por su conflictividad constitucional; ya sea por contraposición con la libertad de expresión —representaciones artísticas, por ejemplo— o por posible derecho penal de autor —punición de la tendencia pederasta—. No obstante, se trata conforme el inc. 4° del Convenio, de dos de los casos en que los estados pueden formular reserva —los otros son el procurarse o procurarle a otro, y la simple posesión de material prohibido—. Corresponde aclarar que, en su segunda reforma del año 2008, en Brasil, se cambió de posición e incluyó la pornografía “virtual” y también la simple tenencia de imágenes como las referidas[268].

Según los fundamentos del Convenio de Budapest, el párrafo 1.b) establece como delito la “oferta” de material de abuso sexual infantil a través de un sistema informático. El término “oferta” se propone abarcar el hecho de pedir a otros que obtengan abuso sexual infantil. Implica que la persona que ofrece el material puede en realidad proporcionarlo. El término “puesta a disposición” se propone abarcar el hecho de poner en línea abuso sexual infantil para que sea utilizada por terceros, por ej., mediante la creación de sitios de abuso sexual infantil. Este párrafo se propone también abarcar la creación o la recopilación de hipervínculos a sitios de abuso sexual infantil con el fin de facilitar el acceso a dichos sitios.

El párrafo 1.c) establece como delito la difusión o la transmisión de abuso sexual infantil a través de un sistema informático. La “difusión” es la diseminación

---

[267] Diario LOS ANDES, “La corte recomienda no usar el termino pornografía infantil”, Url: https://www.losandes.com.ar/la-corte-recomienda-no-usar-el-termino-pornografia-infantil/

[268] RIQUERT, Marcelo Alfredo. “Algo más sobre la Legislación contra la Delincuencia Informática en MERCOSUR a propósito de la Modificación al Código Penal Argentino por Ley 26388”, publicado en AR-DI, Nº 121, Agosto 2008.

activa del material. El hecho de enviar abuso sexual infantil a otra persona a través de un sistema informático estaría comprendido dentro del delito de "transmisión" de abuso sexual infantil.

Quizás el aspecto más discutido (por ejemplo en Argentina), ha sido la punición de la posesión de material de abuso sexual infantil en un sistema informático o en un dispositivo de almacenamiento de datos informáticos. En el fundamento del considerando 98 del Convenio se afirma que "*La posesión de pornografía infantil estimula la demanda de dichos materiales. Una manera eficaz de reducir la producción de pornografía infantil es imponer consecuencias penales a la conducta de cada participante que interviene en la cadena desde la producción hasta la posesión*".

Argentina ha tenido sus idas y vueltas con respecto al tema. En el año 2008, al momento de la sanción de la Ley 26.388, se optó por dejar sin penar la simple posesión, aspecto que en palabras de Gustavo Arocena, "*es merecedor de fundados reproches dogmático-jurídicos por no satisfacer las exigencias elementales del principio de culpabilidad en orden a la necesidad de una acción o una omisión humana como presupuesto para la legítima imposición de una pena. Es que, en definitiva, la expresión "tener" no describe ninguna forma de conducta humana.*"[269]

Sin embargo, años más tarde (2019), el decreto 349/2018 promulgó la ley 27.436 que castiga la simple tenencia de material de abuso sexual infantil.

El nuevo texto de la norma establece que será sancionado con penas de prisión de tres a seis años el que produjere, financiare, ofreciere, comerciare, publicare, facilitare, divulgare o distribuyere, por cualquier medio pornografía infantil.

A diferencia de la anterior escala penal que era de seis meses a cuatro años. Además se reprime con prisión de cuatro meses a un año el que tenga en su poder "representaciones de las descritas en el párrafo anterior", y entre seis meses a dos años para quien tenga material "con fines inequívocos de distribución o comercialización". la sanción también aumentó pero sólo en el mínimo, ya que en el pasado era de cuatro meses a dos años.

[269] AROCENA, G. A. (2012). La regulación de los delitos informáticos en el Código Penal argentino: Introducción a la Ley Nacional núm. 26.388. Boletín mexicano de derecho comparado, 45(135), 945-988.

En relación a este delito, la experta en la materia y fiscal Daniela Dupuy a cargo de la fiscalía especializada en Delitos Informáticos de CABA afirma que: "En poco tiempo, la figura del vendedor de pornografía infantil fue sustituida por la de consumidores que se asocian sin ánimo de lucro, bajando, subiendo y facilitando cantidad de archivos de contenido pornográfico infantil rápidamente y ayudados por las técnicas avanzadas de la tecnología -red peer to peer". Y agrega: "Hoy la situación es incontrolable y es fundamental abordar la problemática desde la prevención, correcta legislación y sin dejar de observar el tratamiento en otros países, pues una de las características fundamentales de los delitos que se llevan a cabo en entornos digitales es la transnacionalidad."[270]

País	Delito 8: Relacionados con Abuso Sexual Infantil
Argentina	**Ley Nº 27.436: ARTICULO 128.-** Será reprimido con prisión de tres (3) a seis (6) años el que produjere, financiare, ofreciere, comerciare, publicare, facilitare, divulgare o distribuyere, por cualquier medio, toda representación de un menor de dieciocho (18) años dedicado a actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales, al igual que el que organizare espectáculos en vivo de representaciones sexuales explícitas en que participaren dichos menores. Será reprimido con prisión de cuatro (4) meses a un (1) año el que a sabiendas tuviere en su poder representaciones de las descriptas en el párrafo anterior. Será reprimido con prisión de seis (6) meses a dos (2) años el que tuviere en su poder representaciones de las descriptas en el primer párrafo con fines inequívocos de distribución o comercialización. Será reprimido con prisión de un (1) mes a tres (3) años el que facilitare el acceso a espectáculos pornográficos o suministrare material pornográfico a menores de catorce (14) años. Todas las escalas penales previstas en este artículo se elevarán en un tercio en su mínimo y en su máximo cuando la víctima fuere menor de trece (13) años.

[270] ERREIUS, Suplemento Especial sobre Cibercrimen y Delitos Informáticos, 2019; Url: https://www.erreius.com/descarga-contenido/Suplemento-Cibercrimen

País	Delito 8: Relacionados con Abuso Sexual Infantil
Brasil	**Ley Nº 11.829 - Art. 241-A.** Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente: Pena – reclusão, de 3 (três) a 6 (seis) anos, e multa. § 1o Nas mesmas penas incorre quem: I – assegura os meios ou serviços para o armazenamento das fotografias, cenas ou imagens de que trata o caput deste artigo; II – assegura, por qualquer meio, o acesso por rede de computadores às fotografias, cenas ou imagens de que trata o caput deste artigo. § 2o As condutas tipificadas nos incisos I e II do § 1o deste artigo são puníveis quando o responsável legal pela prestação do serviço, oficialmente notificado, deixa de desabilitar o acesso ao conteúdo ilícito de que trata o caput deste artigo. **Ley Nº 11.829 - Art. 241-B.** Adquirir, possuir ou armazenar, por qualquer meio, fotografia, vídeo ou outra forma de registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente: Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa. § 1o A pena é diminuída de 1 (um) a 2/3 (dois terços) se de pequena quantidade o material a que se refere o caput deste artigo. § 2o Não há crime se a posse ou o armazenamento tem a finalidade de comunicar às autoridades competentes a ocorrência das condutas descritas nos arts. 240, 241, 241-A e 241-C desta Lei, quando a comunicação for feita por: I – agente público no exercício de suas funções; II – membro de entidade, legalmente constituída, que inclua, entre suas finalidades institucionais, o recebimento, o processamento e o encaminhamento de notícia dos crimes referidos neste parágrafo; III – representante legal e funcionários responsáveis de provedor de acesso ou serviço prestado por meio de rede de computadores, até o recebimento do material relativo à notícia feita à autoridade policial, ao Ministério Público ou ao Poder Judiciário. § 3o As pessoas referidas no § 2o deste artigo deverão manter sob sigilo o material ilícito referido.
Colombia	**CP Art. 218. Pornografía con personas menores de 18 años.** [Modificado por el artículo 24 de la ley 1336 de 2009] El que fotografíe, filme, grabe, produzca, divulgue, ofrezca, venda, compre, posea, porte, almacene, trasmita o exhiba, por cualquier medio, para uso personal o intercambio, representaciones reales de actividad sexual que involucre persona menor de 18 años de edad, incurrirá en prisión de 10 a 20 años y multa de 150 a 1.500 salarios mínimos legales mensuales vigentes. Igual pena se aplicará a quien alimente con pornografía infantil bases de datos de Internet, con o

País	Delito 8: Relacionados con Abuso Sexual Infantil
	sin fines de lucro. La pena se aumentará de una tercera parte a la mitad cuando el responsable sea integrante de la familia de la víctima.
México	**CP. Art. 202** Comete el delito de pornografía de personas menores de dieciocho años de edad o de personas que no tienen capacidad para comprender el significado del hecho o de personas que no tienen capacidad para resistirlo, quien procure, obligue, facilite o induzca, por cualquier medio, a una o varias de estas personas a realizar actos sexuales o de exhibicionismo corporal con fines lascivos o sexuales, reales o simulados, con el objeto de video grabarlos, fotografiarlos, filmarlos, exhibirlos o describirlos a través de anuncios impresos, transmisión de archivos de datos en red pública o privada de telecomunicaciones, sistemas de cómputo, electrónicos o sucedáneos. Al autor de este delito se le impondrá pena de siete a doce años de prisión y de ochocientos a dos mil días multa. A quien fije, imprima, video grabe, fotografíe, filme o describa actos de exhibicionismo corporal o lascivos o sexuales, reales o simulados, en que participen una o varias personas menores de dieciocho años de edad o una o varias personas que no tienen capacidad para comprender el significado del hecho o una o varias personas que no tienen capacidad para resistirlo, se le impondrá la pena de siete a doce años de prisión y de ochocientos a dos mil días multa, así como el decomiso de los objetos, instrumentos y productos del delito. La misma pena se impondrá a quien reproduzca, almacene, distribuya, venda, compre, arriende, exponga, publicite, transmita, importe o exporte el material a que se refieren los párrafos anteriores. **CP Art. 202 BIS.-** Quien almacene, compre, arriende, el material a que se refieren los párrafos anteriores, sin fines de comercialización o distribución se le impondrán de uno a cinco años de prisión y de cien a quinientos días multa. Asimismo, estará sujeto a tratamiento psiquiátrico especializado.
España	**Artículo 189.** 1. Será castigado con la pena de prisión de uno a cinco años: a) El que captare o utilizare a menores de edad o a personas con discapacidad necesitadas de especial protección con fines o en espectáculos exhibicionistas o pornográficos, tanto públicos como privados, o para elaborar cualquier clase de material pornográfico, cualquiera que sea su soporte, o financiare cualquiera de estas actividades o se lucrare con ellas. b) El que produjere, vendiere, distribuyere, exhibiere, ofreciere o facilitare la producción, venta, difusión o exhibición por cualquier medio de pornografía infantil o en cuya elaboración hayan sido utilizadas personas con discapacidad necesitadas de especial protección, o lo poseyere para estos fines, aunque el material tuviere su origen en el extranjero o fuere desconocido.

País	Delito 8: Relacionados con Abuso Sexual Infantil
	A los efectos de este Título se considera pornografía infantil o en cuya elaboración hayan sido utilizadas personas con discapacidad necesitadas de especial protección: a) Todo material que represente de manera visual a un menor o una persona con discapacidad necesitada de especial protección participando en una conducta sexualmente explícita, real o simulada. b) Toda representación de los órganos sexuales de un menor o persona con discapacidad necesitada de especial protección con fines principalmente sexuales. c) Todo material que represente de forma visual a una persona que parezca ser un menor participando en una conducta sexualmente explícita, real o simulada, o cualquier representación de los órganos sexuales de una persona que parezca ser un menor, con fines principalmente sexuales, salvo que la persona que parezca ser un menor resulte tener en realidad dieciocho años o más en el momento de obtenerse las imágenes. d) Imágenes realistas de un menor participando en una conducta sexualmente explícita o imágenes realistas de los órganos sexuales de un menor, con fines principalmente sexuales. 2. Serán castigados con la pena de prisión de cinco a nueve años los que realicen los actos previstos en el apartado 1 de este artículo cuando concurra alguna de las circunstancias siguientes: a) Cuando se utilice a menores de dieciséis años. b) Cuando los hechos revistan un carácter particularmente degradante o vejatorio, se emplee violencia física o sexual para la obtención del material pornográfico o se representen escenas de violencia física o sexual. c) Cuando se utilice a personas menores de edad que se hallen en una situación de especial vulnerabilidad por razón de enfermedad, discapacidad o por cualquier otra circunstancia. d) Cuando el culpable hubiere puesto en peligro, de forma dolosa o por imprudencia grave, la vida o salud de la víctima. e) Cuando el material pornográfico fuera de notoria importancia. f) Cuando el culpable perteneciere a una organización o asociación, incluso de carácter transitorio, que se dedicare a la realización de tales actividades. g) Cuando el responsable sea ascendiente, tutor, curador, guardador, maestro o cualquier otra persona encargada, de hecho, aunque fuera provisionalmente, o de derecho, de la persona menor de edad o persona con discapacidad necesitada de especial protección, o se trate de cualquier persona que conviva con él o de otra persona que haya actuado abusando de su posición reconocida de confianza o autoridad. h) Cuando concurra la agravante de reincidencia. 3. Si los hechos a que se refiere la letra a) del párrafo primero del apartado 1 se hubieran cometido con violencia o intimidación se impondrá la pena superior en grado a las previstas en los apartados anteriores.

País	Delito 8: Relacionados con Abuso Sexual Infantil
	4. El que asistiere a sabiendas a espectáculos exhibicionistas o pornográficos en los que participen menores de edad o personas con discapacidad necesitadas de especial protección, será castigado con la pena de seis meses a dos años de prisión. 5. El que para su propio uso adquiera o posea pornografía infantil o en cuya elaboración se hubieran utilizado personas con discapacidad necesitadas de especial protección, será castigado con la pena de tres meses a un año de prisión o con multa de seis meses a dos años. La misma pena se impondrá a quien acceda a sabiendas a pornografía infantil o en cuya elaboración se hubieran utilizado personas con discapacidad necesitadas de especial protección, por medio de las tecnologías de la información y la comunicación. 6. El que tuviere bajo su potestad, tutela, guarda o acogimiento a un menor de edad o una persona con discapacidad necesitada de especial protección y que, con conocimiento de su estado de prostitución o corrupción, no haga lo posible para impedir su continuación en tal estado, o no acuda a la autoridad competente para el mismo fin si carece de medios para la custodia del menor o persona con discapacidad necesitada de especial protección, será castigado con la pena de prisión de tres a seis meses o multa de seis a doce meses. 7. El Ministerio Fiscal promoverá las acciones pertinentes con objeto de privar de la patria potestad, tutela, guarda o acogimiento familiar, en su caso, a la persona que incurra en alguna de las conductas descritas en el apartado anterior. 8. Los jueces y tribunales ordenarán la adopción de las medidas necesarias para la retirada de las páginas web o aplicaciones de internet que contengan o difundan pornografía infantil o en cuya elaboración se hubieran utilizado personas con discapacidad necesitadas de especial protección o, en su caso, para bloquear el acceso a las mismas a los usuarios de Internet que se encuentren en territorio español. Estas medidas podrán ser acordadas con carácter cautelar a petición del Ministerio Fiscal.

Tabla Nº 11: Cuadro comparativo de tipificación de Delito 8: Material de Abuso Sexual Infantil

4.6.11. Delito 9: Suplantación de identidad digital

La conducta básica refiere a quien sin consentimiento, adquiriera, tuviere en posesión, transfiriera, creare o utilizare la identidad de una persona física o jurídica, a través de cualquier medio electrónico.

Alternativamente se establecen como elementos del tipo penal la intención de dañar, o la efectiva realización de un daño, o la obtención de algún beneficio para sí o para terceros.

Su justificación tiene relación con considerar una mayor protección al derecho a la identidad de las personas. En Argentina se han presentado distintos proyectos de Ley tendientes a su incorporación como delito autónomo, uno de los cuáles este autor ha formado parte[271], escribiendo artículos al respecto[272].

Para analizar estas actividades es importante destacar la diferencia entre la suplantación de identidad digital y la "impersonalización", que sucede simplemente cuando alguien se hace pasar por otra persona u organización. Si bien en la mayoría de los casos el suplantación de identidad se basa en la impersonalización para efectuar una acción delictiva, puede suceder que la impersonalización sólo se realice con "fines más inocentes" como puede ser hacerse pasar por un famoso, hablar en nombre de otro o intentar obtener descuentos utilizando su identidad.

Desde el punto de vista del bien jurídico protegido, entendemos que se trata de la identidad de las personas, en su faceta "dinámica". Un importante fallo italiano[273] expresó que la identidad era "el conjunto de atributos, calidades, caracteres y acciones que distinguen a un individuo con respecto a cualquier otro, y que conforma su derecho a ser reconocido en su 'peculiar realidad'". Sobre esta línea, el jurista peruano Fernando Sessarego[274], supo dotar de mayor precisión al concepto buscado, afirmando que se trataba de un conjunto de atributos y características que permiten individualizar a la persona en sociedad, donde ese ese plexo de características de la personalidad de cada cual se proyecta hacia el mundo exterior y permite a los demás conocer a la persona, a "cierta persona", en su "mismidad", en lo que ella es en cuanto particular y específico ser humano.

Como se puede observar, se trata de un concepto que no se limita a considerar el aspecto físico o biológico de la persona; comprende también el aspecto espiritual,

---

[271] HONORABLE SENADO DE LA NACIÓN ARGENTINA, Proyecto Nº 1312/12 de ley Presentado ante el Honorable Congreso de la Nación. Ingresado en fecha 15/05/2012, Url: http://www.senado.gov.ar/web/proyectos/verExpe.php?origen=S&tipo=PL&numexp=1312/12&nro_comision=&tConsulta=1

[272] TEMPERINI, Marcelo y BORGHELLO, Cristian, "Suplantación de Identidad Digital como delito informático". Doctrina publicada en el Libro "Cibercrimen: aspectos de Derecho penal y procesal penal. Cooperación internacional. Recolección de evidencia digital. Responsabilidad de los proveedores de servicios de internet". Directora: Daniela Dupuy. ISBN: 9789974745063; Editorial: Editorial B de f; 2016.

[273] Corte Suprema italiana, 13 VII 71, Foro Italiano, 1972 I 432

[274] Fernández Sessarego, C. (1992). Derecho a la identidad personal. Buenos Aires: Astrea, 113.

intelectual, religioso, social, profesional, psicológico, a través del cual el individuo se proyecta socialmente al exteriorizar de alguna manera esos aspectos propios de su personalidad. Por eso en doctrina[275] se ha señalado desde hace tiempo que puede hablarse de una doble faz en la identidad personal: la estática, que apunta a los rasgos físicos y biológicos del individuo, inmutables por naturaleza, y la dinámica que se refiere a los modos particulares que ese sujeto adopta para comunicarse e insertarse en su vida de relación con los demás.

Más allá de las posibles pérdidas financieras y económicas directas (afectación del patrimonio como bien jurídico), aspecto que estaría penalmente cubierto por el delito de estafa, también existen otros tipos de daños que pueden ser causados a las víctimas de una suplantación de identidad digital. Entre esas posibilidades, se encuentran los daños al buen nombre, la imagen, la honra y la reputación de la víctima.

El principal inconveniente para la persona afectada está asociado al impacto social, psicológico y moral que implica que su identidad pueda ser utilizada por un tercero. Dicho efecto es producido como consecuencia de que el delincuente, al suplantar la identidad digital de la víctima, ocasiona en ella un daño hacia su identidad que podrá ser más o menos dañoso de acuerdo al caso.

En el derecho comparado se puede encontrar diferentes tipos de estrategias legales frente a esta figura delictiva. Algunos países, como Estados Unidos y Canadá, poseen regulaciones generales para el "*identity theft*", adaptados de tal manera que el mismo tipo penal es aplicable tanto para el "robo de identidad" clásico, así como para el robo de identidad digital. A su vez, ambos completan su esquema a través de la tipificación de la tenencia ilegítima de datos de identificación personal, así como del tráfico (sin consentimiento) de estos datos. En Argentina, existieron distintas resistencias con respecto a reconocer el concepto de "robo de identidad"[276], entendiendo que técnicamente no es posible "robarla" (en el sentido penal de existir fuerza o violencia en las cosas), por eso se ha considerado más apropiado seguir la línea americana, de considerar que existe una suplantación.

[275] CABRERA, Delma Y CODEGLIA, Luis María, "Responsabilidad por violación al derecho a la identidad". Publicado en "La responsabilidad (Homenaje al profesor Doctor Isidoro H. Goldenberg)". 1ra. edición, 1995

[276] Temática sobre la cual ha trabajando incansablemente el Dr. Monastersky, a través de distintas propuestas legislativas.

Estados Unidos, a nivel federal lo define como el que "a sabiendas, posea, transfiera o use, sin autoridad legal, un medio de identificación de otra persona con la intención de cometer, ayudar o instigar, cualquier tipo de actividad ilegal". Luego, algunos Estados como New York[277], tienen un completo desarrollo en la materia, puntualmente como derivaciones de su artículo 190 (other frauds), donde por ejemplo el art. 190.25 (Criminal impersonation in the second degree), tipifica a quien "usurpa la identidad de otro a través de internet o medios electrónicos, con la intención de obtener un beneficio o injuriar o defraudar a otro...". Se debe destacar que en todas estas regulaciones, más allá del tipo penal objetivo -hacerse pasar por otro utilizando medios electrónicos-, incluyen el aspecto subjetivo, destacando que para que exista delito, debe también existir la intención de obtener beneficio, dañar, defraudar, injuriar, etc. No obstante esta tipificación, en el 2011 se presentó un proyecto en el Senado de New York para agregar un tipo penal nuevo (el art. 190.87) cuya redacción es aún más precisa en el aspecto subjetivo del tipo penal. Completando la seriedad de su regulación, New York posee tipos específicos para la tenencia ilegítima de datos de identificación personal (art. 190.81/2/3 Unlawful possession of personal identification), así como prevé casos especiales para exclusión del tipo (art. 190.84, donde por ejemplo, excluye a los jóvenes menores de 21 años que se hagan pasar por mayores para comprar alcohol).

Como se ha podido observar a lo largo de este subcapítulo, la identidad digital es susceptible de ser afectada por personas que realizan suplantación de

[277] S 190.80 Identity theft in the first degree. A person is guilty of identity theft in the first degree when he or she knowingly and with intent to defraud assumes the identity of another person by presenting himself or herself as that other person, or by acting as that other person or by using personal identifying information of that other person, and thereby: 1. obtains goods, money, property or services or uses credit in the name of such other person in an aggregate amount that exceeds two thousand dollars; or 2. causes financial loss to such person or to another person or persons in an aggregate amount that exceeds two thousand dollars; or 3. commits or attempts to commit a class D felony or higher level crime or acts as an accessory in the commission of a class D or higher level felony; or 4. commits the crime of identity theft in the second degree as defined in section 190.79 of this article and has been previously convicted within the last five years of identity theft in the third degree as defined in section 190.78, identity theft in the second degree as defined in section 190.79, identity theft in the first degree as defined in this section, unlawful possession of personal identification information in the third degree as defined in section 190.81, unlawful possession of personal identification information in the second degree as defined in section 190.82, unlawful possession of personal identification information in the first degree as defined in section 190.83, unlawful possession of a skimmer device in the second degree as defined in section 190.85, unlawful possession of a skimmer device in the first degree as defined in section 190.86, grand larceny in the fourth degree as defined in section 155.30, grand larceny in the third degree as defined in section 155.35, grand larceny in the second degree as defined in section 155.40 or grand larceny in the first degree as defined in section 155.42 of this chapter. Identity theft in the first degree is a class D felony. New York State Law. Penal Laws. Article 190.80, "Other frauds"; http://ypdcrime.com/penal.law/article190.htm.

identidades digitales. Aún existen discusiones si dicha afectación implica el merecimiento de la intervención penal. Para estos casos, consideramos que podría (como se ha sugerido en varios de los delitos clásicos vistos anteriormente, la inclusión de la gravedad en la consecuencia disvaliosa).

Participamos de un sector que considera apropiado aunar esfuerzos hacia el futuro, buscando la defensa de las personas afectadas, generando una propuesta para que se considere a la identidad digital como un bien jurídico protegido. En este sentido, consideramos necesaria la tipificación de la suplantación de identidad digital, proponiendo la siguiente fórmula al respecto para Argentina (país donde ya adelantamos que no existe tipificación al respecto).

> *Art. 138 bis: Será reprimido con prisión de multa de [.....] pesos, el que sin consentimiento utilizare la identidad de una persona física o jurídica que no le pertenezca, a través de cualquier medio, y con la intención de dañar, extorsionar, defraudar, injuriar o amenazar a otra persona u obtener beneficio para sí o para terceros.*

Como cierre destacamos que una adecuada legislación siempre es necesaria, pero no es suficiente. Junto con ella, deberá establecerse un centro de atención a las víctimas, con personal capacitado y con los recursos suficientes para poder, en la práctica, darle eficacia a la normativa realizando una real detección, investigación y persecución de estos delitos informáticos. Por último, insistir en que es fundamental la realización de campañas de capacitación y concientización a los usuarios con relación a buenas prácticas en materia de seguridad de la información.

País	Delito 9: Suplantación de Identidad Digital
Argentina	**Parcialmente aplicable. Código Contravencional de CABA: (No regulado en Código Penal). Articulo 68 quinquies. Suplantación digital de la Identidad.** Quien utiliza la imagen y/o datos filiatorios de una persona o crea una identidad falsa con la imagen y/o datos filiatorios de una persona mediante la utilización de cualquier tipo de comunicación electrónica, transmisión de datos, página web y/o cualquier otro medio y se haya realizado sin mediar consentimiento de la víctima, siempre que el hecho no constituya delito, es sancionado con una multa de Ciento sesenta (160) a cuatrocientas (400) unidades fijas o uno (1) a cinco (5) días de trabajo de utilidad pública o de uno (1) a cinco (5) días de arresto. Las sanciones se elevan al doble cuando: La conducta sea realizada con la finalidad de realizar un banco de datos con la información obtenida. La víctima fuera menor de dieciocho (18) años, mayor de 70 años, o con discapacidad. La contravención sea cometida por el/la cónyuge, ex cónyuge, o a la persona con quien mantiene o ha mantenido una relación de pareja, mediare o no convivencia. La contravención sea cometida por un familiar de hasta el cuarto grado de consanguinidad o segundo grado de afinidad. La contravención sea cometida con el objeto de realizar una oferta de servicios sexuales a través de cualquier medio de comunicación. El consentimiento de la víctima, siendo menor de 18 años, no será considerado válido. Acción dependiente de instancia privada con excepción de los casos donde la víctima fuere menor de 18 años de edad. No configura suplantación de identidad el ejercicio del derecho a la libertad de expresión. (Conforme texto Art. 6º de la Ley Nº 6.128, BOCBA N° 5531 del 07/01/2019)
Brasil	No se encontró tipificación.
Colombia	**Parcialmente aplicable. CP Art. 296. Falsedad personal.** El que con el fin de obtener un provecho para sí o para otro, o causar daño, sustituya o suplante a una persona o se atribuya nombre, edad, estado civil, o calidad que pueda tener efectos jurídicos, incurrirá en multa, siempre que la conducta no constituya otro delito. **Parcialmente aplicable. Artículo 269G: Suplantación de sitios web para capturar datos personales.** El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave. En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a

País	Delito 9: Suplantación de Identidad Digital
	otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave. La pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito.
México	No se encontró tipificación.
España	**Parcialmente aplicable. Artículo 401.** El que usurpare el estado civil de otro será castigado con la pena de prisión de seis meses a tres años.

Tabla Nº 12: Cuadro comparativo de tipificación de Delito 9: Suplantación de Identidad Digital

4.6.12. Delito 10: Captación ilegítima de datos confidenciales (Phishing)

La conducta básica del phishing (pesca de datos) refiere a quien mediante cualquier forma de ardid o engaño, indebidamente obtuviere o captare datos confidenciales.

A fines académicos, recordamos que la figura del phishing es autónoma y no necesariamente implica la realización de una posterior estafa económica (asociado al phishing bancario), ya que dicha captación ilegítima podría tener como pasos posteriores distintas opciones.

La primera cita a la palabra “phishing” se puede encontrar en el popular grupo de noticias de hacking alt.2600 en enero de 1996, cuando varios delincuentes obtuvieron datos y contraseñas de usuarios de AOL (America On Line). Este vocablo “phishing” fue acuñado por ser la contracción de “Password Harvesting Fishing”, literalmente “cosecha y pesca de contraseñas”, donde se destaca que en su propio nombre no se menciona el método ni el objetivo para el cual esos datos son recolectados.

En 1997, esta técnica ya era ampliamente conocida y utilizada para obtener datos y comercializarlos en el mercado negro. En todos los casos analizados, se hace referencia al uso de técnicas de ingeniería social, donde se engaña y manipula psicológicamente a la víctima para que revele datos que no brindaría en circunstancias normales (lure). En estos casos, el engaño se efectúa a través del uso de cualquier medio de comunicación tecnológico como el teléfono, fax, correo electrónico, chat, SMS, etc. Más allá de lo expuesto, cabe aclarar que la dificultad en la conceptualización de esta técnica, viene relacionado a que su práctica y caracterización ha ido mutando constantemente.

Atento a ello, y en la búsqueda de encontrar una clasificación que permita mejorar la comprensión de estos delitos, se pueden distinguir dos fases perfectamente diferenciadas.

La primera fase consta de la obtención de información confidencial o sensible del usuario a través de distintas técnicas. En este caso el delincuente toma contacto con la víctima a través de cualquier medio de comunicación y, con un componente de ingeniería social, engaña al usuario para que entregue voluntariamente la información solicitada (nombres de usuario, contraseña, números de cuenta, PIN, tarjetas de crédito, token de whatsapp, etc.).

Hace no tantos años, la forma más tradicional de llevar adelante esta etapa es realizar el envío masivo de correo electrónico no deseado -spam- a miles o millones de direcciones previamente recolectadas para lograr, posteriormente, que el usuario ingrese a un sitio web similar al de una entidad de confianza y coloque allí la información necesaria para concretar la segunda etapa.

Si bien una importante cantidad de casos busca obtener los datos financieros de la víctima (para concretar futuras estafas), vale destacar que esta primera fase no debe considerarse como asociada o vinculada exclusivamente al fraude informático, error muy común en el ámbito de los delitos informáticos.

Esta etapa inicial de captación ilegítima de datos, puede ser utilizada para obtener cualquier tipo de información de utilidad para el delincuente, tales como datos de autenticación (login), datos de una cuenta de red social, blog, cuenta bancaria o casilla de correo, incluso hasta información más puntual, como los

secretos industriales de una empresa, que son obtenidos por el delincuente mediante trampas (engaños/lure) especialmente diseñadas para esos fines.

Concluida la primera etapa de captación de los datos del usuario, se procede a una segunda etapa, donde el delincuente se encuentra con un espectro de posibilidades diversas. Si bien como mencionamos, las estadísticas demuestran que tradicionalmente aquí el delincuente comienza a utilizar los datos obtenidos para obtener beneficios económicos perjudicando el patrimonio de la víctima, con el tiempo la actividad se ha ido desprendiendo de esta finalidad casi exclusiva, existiendo en la actualidad un crecimiento de las otras opciones que se pueden realizar con los datos captados. Aquí presentamos un listado de las opciones mencionadas:

- Venta de la información obtenida a otros delincuentes en el mercado negro. En este caso la información cotiza de acuerdo al grado de plenitud y exactitud (no es lo mismo una base de datos con el nombre de usuario y contraseña que aquella que además contiene el número de tarjeta de crédito y su PIN). *Esta actividad no se encuentra tipificada actualmente en Argentina.*
- Extracción directa de dinero de las cuentas obtenidas. Esta actividad si se encuentra tipificada en Argentina (art. 173 inc. 16 CP) y es la calificada como "fraude informático". A su vez, reviste diferentes opciones:
    - Realización de transferencias de manera directa por el delincuente a cuentas propias (poco frecuente por su posibilidad de rastreo).
    - Utilización de "mulas", aquellas personas que, de forma inocente y generalmente sin conocimiento, facilitan su cuenta bancaria para realizar movimientos de dinero obtenido de transacciones fraudulentas. Actualmente, la facilidad para abrir "billeteras virtuales", facilita la generación de CBU/CVU temporales funcionales a este tipo de maniobras.
- Adquisición de bienes o servicios a través de canales virtuales que no soliciten la presencia del titular o de su documentación. En este tipo de fraude es común la compra de créditos para líneas de teléfono móvil. Esta actividad se encuentra tipificada en Argentina (art. 173 inc. 16 CP).

- Ejecución de una "broma" a la víctima, donde se establecen comunicaciones o se generan perfiles falsos en su nombre. Esta actividad es muy común en los jóvenes y es generalmente llevada a cabo en las redes sociales y chats. No se encuentra tipificada en Argentina (aunque podría existir el delito de injurias para casos graves).
- Suplantación de identidad de la víctima, provocando un daño personal -injuria, daños a la reputación, lesión al honor- en nombre de la víctima. Esta actividad no se encuentra tipificada en Argentina, excepto para casos de estafa, que opera como delito autónomo (ver delito anterior de esta tesis).
- Publicación de la información obtenida en Internet. En ocasiones, el delincuente se limita a captar ilegítimamente los datos para posteriormente "colgarlos" en la red, a sabiendas que su difusión generará consecuencias en los medios y en la opinión pública sobre la empresa u organismo encargado de la seguridad de esos datos.
- Extorsión. El delincuente realiza la captación ilegítima de datos, para posteriormente contactar amenazando con la difusión de la información confidencial obtenida.
- Colección personal. Pueden existir casos donde el sujeto que capto la información, decida no utilizar en ninguna de las alternativas descriptas, limitándose a recolectarlas de manera privada sin posterior uso.
- Venta de información. Una de las alternativas más probables del actual ecosistema del cibercrimen, donde los grupos criminales que logran hacerse con información de cierto interés o valor, la ofrecen en el mercado negro al mejor postor. Un claro ejemplo recién, ha sido el ofrecimiento de la base de datos de RENAPER[278].

En orden a lo desarrollado sobre la primera y segunda etapa de esta actividad, nos encontramos ya en condiciones de poder desarrollar un concepto sobre lo que debemos considerar como phishing. De acuerdo a nuestra posición, debe

[278] Diario La Nación; "Preocupación por la venta online de los datos de los argentinos que tiene el Registro Nacional de las Personas", Url: https://www.lanacion.com.ar/tecnologia/preocupacion-por-la-venta-de-los-datos-de-millones-de-argentinos-que-tiene-el-registro-nacional-de-nid13102021/

considerarse "phishing" a la práctica de la obtención ilegítima de datos confidenciales, independientemente de la opción que se busque realizar en una segunda etapa con esos datos.

Es decir, consideramos que el phishing existe de manera plena y completa dentro de la primera fase ya explicada, independientemente de la actividad posterior que realice el delincuente. Definida la clasificación de las etapas, se hace imprescindible el análisis profundo de los motivos del robo de información y el debate sobre la necesidad de tipificación de la captura ilegítima de datos confidenciales, concebida como acto preparatorio raíz de diferentes tipos de problemas.

A modo local, hemos tenido la oportunidad de participar en la producción de un proyecto de ley al respecto al cual remitimos en honor a la brevedad[279], que propone la tipificación de dicha actividad a través de la siguiente fórmula penal:

> *ARTICULO 157 ter. - Será reprimido con multa de pesos [.....] a pesos [.....] el que de forma deliberada e ilegítima:*
>
> *1. Mediante cualquier forma de ardid o engaño, indebidamente obtuviere o captare datos personales, financieros o confidenciales*
>
> *2. Con fines ilícitos, diseñare, programare, desarrollare, vendiere, ejecutare, facilitare o enviare un dispositivo, sistema o programa informático, destinados a la indebida obtención o captura de datos personales, financieros o confidenciales.*

De los tipos penales analizados anteriormente, como ya lo hemos señalado, entendemos que la figura penal sugerida por el Convenio de Budapest que más se aproxima a esta conducta, tiene asidero legal en una de las combinaciones posibles del abuso de dispositivos. En particular, al sugerir la penalización de:

"La comisión deliberada e ilegítima de la producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de una

[279] Presentado ante el Honorable Congreso de la Nación. Ingresado en fecha 09/09/2011, Expediente Nro. 2257/11; Url; http://www.senado.gov.ar/web/proyectos/verExpe.php?origen=S&tipo=PL&numexp=2257/11&nrocomision=&tConsulta=1

contraseña, un código de acceso o datos informáticos similares que permitan tener acceso a la totalidad o a una parte de un sistema informático, con el fin de que sean utilizados para la comisión de cualquiera de los delitos contemplados en los artículos 2 a 5; y b)"[280]

País	Delito 10: Captación ilegítima de datos (Phishing)
Argentina	**Parcialmente aplicable. Ley 26.388 - Artículo 157 bis:** Será reprimido con la pena de prisión de un (1) mes a dos (2) años el que: 1. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales; 2. Ilegítimamente proporcionare o revelare a otro información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley. 3. Ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales.
Brasil	No se encontró tipificación.
Colombia	**Art. 269G. Suplantación de sitios web para capturar datos personales.** El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave. En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave. La pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito.
México	No se encontró tipificación.

[280] Art. 6 del Convenio de Cibercrimen de Budapest, inc. 1 a ii.

País	Delito 10: Captación ilegítima de datos (Phishing)
España	**Artículo 249.** 1. También se consideran reos de estafa y serán castigados con la pena de prisión de seis meses a tres años: a) Los que, con ánimo de lucro, obstaculizando o interfiriendo indebidamente en el funcionamiento de un sistema de información o introduciendo, alterando, borrando, transmitiendo o suprimiendo indebidamente datos informáticos o valiéndose de cualquier otra manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro. b) Los que, utilizando de forma fraudulenta tarjetas de crédito o débito, cheques de viaje o cualquier otro instrumento de pago material o inmaterial distinto del efectivo o los datos obrantes en cualquiera de ellos, realicen operaciones de cualquier clase en perjuicio de su titular o de un tercero. 2. Con la misma pena prevista en el apartado anterior serán castigados: a) Los que fabricaren, importaren, obtuvieren, poseyeren, transportaren, comerciaren o de otro modo facilitaren a terceros dispositivos, instrumentos o datos o programas informáticos, o cualquier otro medio diseñado o adaptado específicamente para la comisión de las estafas previstas en este artículo. b) Los que, para su utilización fraudulenta, sustraigan, se apropiaren o adquieran de forma ilícita tarjetas de crédito o débito, cheques de viaje o cualquier otro instrumento de pago material o inmaterial distinto del efectivo. 3. Se impondrá la pena en su mitad inferior a los que, para su utilización fraudulenta y sabiendo que fueron obtenidos ilícitamente, posean, adquieran, transfieran, distribuyan o pongan a disposición de terceros tarjetas de crédito o débito, cheques de viaje o cualesquiera otros instrumentos de pago materiales o inmateriales distintos del efectivo.

Tabla Nº 13: Cuadro comparativo de tipificación de Delito 10: Captación Ilegítima de Datos (Phishing)

4.6.13. Delito 11: Violación de datos personales

La conducta básica refiere a quien a través de cualquier medio, publicare indebidamente o sin consentimiento datos personales -información confidencial-. En este contexto, remitidos al desarrollo realizado en el Capítulo 2, entendiendo que la confidencialidad de la información, es la características más genérica que protege

todo tipo de información de su divulgación indebida (ya sea relativa a secretos comerciales, o bien, a información privada o íntima de una persona).

Si bien entendemos que la regulación sobre difusión de información confidencial suele ser más clásica, existente desde hace años en los distintos ordenamientos penales, su lógica de protección era distinta, pretendía proteger más bien el valor comercial de dicha información que otros aspectos de la misma.

En el escenario actual, la proliferación de casos de los (mal) llamados "revenge porn", o difusión no consentida de imágenes de la intimidad (o violencia de género digital), ha dado lugar a un fenómeno de regulación en distintos lugares del mundo, que nos parece de interés, incorporar su realidad a nivel latinoamericano.

Advertimos que el desarrollo de la presente figura, importaría realizar un capítulo completo de esta tesis y no es el objetivo buscado. Aquí pretendemos presentar la figura como introducción al trabajo de derecho comparado que venimos realizando, tratando de visibilizar la existencia de conductas más "novedosas" que aún en la mayoría de los países, no encuentra reconocimiento penal.

Comenzaremos abordando que la denominación "revenge porn" tiene relación con casos donde por venganza se difunden las imágenes de contenido sexual de la ex pareja, con la que voluntariamente se había compartido o se había consentido su captación durante la relación íntima. Por un lado debemos considerar que no todos los sujetos activos de este delito podrán actuar por venganza y por otro, que las imágenes de relaciones privadas no son per se pornográficas, por lo que no estamos de acuerdo con la utilización de dicho término, considerando mucho más apropiado denominarlo como "difusión no consentida de contenidos o material de la intimidad".

En su esencia, la difusión no consentida de material íntimo es un delito contra la privacidad. La acción típica consiste en difundir contra la voluntad de la víctima material (video, fotos, audios) de escenas muy privadas o íntimas (en general de contenido sexual), que inicialmente fueron captadas con su consentimiento, y que luego se difunden contra su voluntad.

La problemática se ha visto incrementada en situación de pandemia, sufriendo un crecimiento exponencial, profundizado en estos dos últimos años por la situación de Emergencia Sanitaria Mundial (COVID-19). En Argentina, el Gobierno

públicamente realizó comunicaciones alentando a la población a no salir de su casa, y de practicar sexo virtual (sexting)[281].

En 2023 en Argentina se aprobó la llamada Ley Olimpia, que incluye a la violencia digital entre las modalidades de violencia contra las mujeres de la Ley 26.485 e incorpora como objeto de la ley el respeto de la "dignidad, reputación e identidad, incluso en los espacios digitales".

La definición de la norma establece que se entiende por violencia digital o telemática "toda conducta, acción u omisión en contra de las mujeres basada en su género que sea cometida, instigada o agravada, en parte o en su totalidad, con la asistencia, utilización y/o apropiación de las tecnologías de la información y la comunicación, con el objeto de causar daños físicos, psicológicos, económicos, sexuales o morales tanto en el ámbito privado como en el público a ellas o su grupo familiar".

Sin embargo, la tipificación penal de este tipo de violencia de género aún se encuentran en estado de proyectos de ley[282]. Se presentó y aprobó (media sanción) en el Senado de la Nación Argentina el 9 de junio de 2016 firmado por las Senadoras Marina Riofrio, Beatriz Mirkin y Norma Durango. El mismo propuso incorporar un nuevo artículo 155 bis al Código Penal argentino (CPen.).

La propuesta con media sanción dice así:

> *"Será reprimido con la pena de prisión de seis (6) meses a cuatro (4) años, el que hallándose en posesión de imágenes de desnudez total o parcial y/o videos de contenido sexual o erótico de una o más personas, las hiciere pública o difundiere por medio de comunicaciones electrónicas, telecomunicaciones, o cualquier otro medio o tecnología de transmisión de datos, sin el expreso consentimiento de la o de las mismas para tal fin, aun habiendo existido acuerdo entre las partes involucradas para la obtención o suministro de esas imágenes o video.*
>
> *La persona condenada será obligada a arbitrar los mecanismos necesarios para retirar de circulación, bloquear, eliminar o suprimir, el material de que se tratare, a su costa y en un plazo a determinar por el juez".*

---

[281] Diario El País, "El Gobierno argentino recomienda el sexo virtual durante la cuarentena obligatoria", Url:https://elpais.com/sociedad/2020-04-17/el-gobierno-argentino-recomienda-el-sexo-virtual-durante-la-cuarentena-obligatoria.html

[282] Proyecto de ley de la Senadora Riofrio, Expediente n. 2119/16 del Senado de la Nación

Dicho proyecto ha recibido distintas críticas y consideraciones, en particular, del maestro Pablo Palazzi[283], quien ha estudiado con profundidad de la temática en nuestro país[284].

Por otro lado, en el 2020 se estuvo debatiendo el Proyecto de Reforma del Código Penal[285] el que establece:

> "*Se impondrá prisión de SEIS (6) meses a DOS (2) años o SEIS (6) a VEINTICUATRO (24) días-multa, al que sin autorización de la persona afectada difundiere, revelare, enviare, distribuyere o de cualquier otro modo pusiere a disposición de terceros imágenes o grabaciones de audio o audiovisuales de naturaleza sexual, producidas en un ámbito de intimidad, que el autor hubiera recibido u obtenido con el consentimiento de la persona afectada, si la divulgación menoscabare gravemente su privacidad.*
>
> *La pena será de prisión de UNO (1) a TRES (3) años:*
>
> *1°) Si el hecho se cometiere por persona que esté o haya estado unida a la víctima por matrimonio, unión convivencial o similar relación de afectividad, aun sin convivencia.*
>
> *2°) Si la persona afectada fuere una persona menor de edad.*
>
> *3°) Si el hecho se cometiere con fin de lucro.*"

Otra referencia en Argentina sobre la consideración de esta figura, es dentro del Código Contravencional de Ciudad Autónoma de Buenos Aires, donde en el Capítulo V, sobre "IDENTIDAD DIGITAL DE LAS PERSONAS", se regula:

> *Artículo 68 bis - Difusión no autorizada de imágenes o grabaciones íntimas. Quien difunda, publique, distribuya, facilite, ceda y/o entregue a terceros imágenes, grabaciones y/o filmaciones de carácter íntimo sin el consentimiento de la persona y a través de cualquier tipo de comunicación electrónica, de trasmisión de datos, páginas web y/o a través de cualquier otro medio de comunicación, siempre que el hecho no constituya delito, es sancionado con una multa de cuatrocientas (400) a mil novecientas cincuenta (1950) unidades fijas o cinco (5) a quince (15) días de trabajo de utilidad pública o con tres (3) a diez (10) días de arresto. El consentimiento de la víctima para la difusión, siendo menor de 18 años, no será considerado válido.*

---

[283] Palazzi, Pablo. (2017). Consideraciones sobre la aprobación por el Senado de un proyecto de ley para penalizar la publicación de imágenes íntimas (revenge porn). El Derecho 19 de abril de 2017.

[284] Palazzi, P. (2016). Difusión no autorizada de imágenes íntimas (revenge porn). Revista El Derecho, 1(1), 1-32.

[285] https://www.argentina.gob.ar/justicia/nuevocodigopenal

Tampoco podrá alegarse el consentimiento de la víctima en la generación del contenido como defensa a la realización de la presente conducta.

Acción dependiente de instancia privada con excepción de los casos donde la víctima sea menor de 18 años de edad.

No configura contravención el ejercicio del derecho a la libertad de expresión.

En relación al bien jurídico afectado, Palazzi[286] sostiene que la difusión de estas imágenes o grabaciones que son privadas, constituyen una afectación de su derecho a la imagen, y en forma más general de su derecho a la intimidad. Así lo han catalogado la reforma del Código penal español del año 2015, incluyéndolo como un nuevo inciso del art. 197[287] (delitos contra la privacidad y violación de secretos) y la reforma del Código Penal francés, que lo incluye en el art. 226-2 del Código Penal francés dentro de la sección dedicada a delitos contra la vida privada.

Dentro del bien jurídico "vida privada" (insertado como título por la ley 26.388) podríamos también entrar en clasificaciones y en este caso es posible sostener que esta figura se trata de un atentado contra la privacidad sexual de la víctima, posiblemente uno de los ámbitos más reservados e importantes de la vida privada que puede tener una persona junto con su pensamiento y sus creencias.[288]

Las Dras. María Florencia Zerdá y Marina Benítez Demtschenko, en un importante trabajo que han realizado[289], postulan puntualmente si es posible considerar que la difusión no consentida de material digital íntimo, la sextorsión, la suplantación de identidad y el acoso virtual son un modo de ejercer violencia de género.

---

[286] PALAZZI, Pablo. (2017). Consideraciones sobre la aprobación por el Senado de un proyecto de ley para penalizar la publicación de imágenes íntimas (revenge porn). El Derecho 19 de abril de 2017.

[287] La reforma modificó el art. 197 con un nuevo inciso séptimo que dice así "Será castigado con una pena de prisión de tres meses a un año o multa de seis a doce meses el que, sin autorización de la persona afectada, difunda, revele o ceda a terceros imágenes o grabaciones audiovisuales de aquélla que hubiera obtenido con su anuencia en un domicilio o en cualquier otro lugar fuera del alcance de la mirada de terceros, cuando la divulgación menoscabe gravemente la intimidad personal de esa persona. La pena se impondrá en su mitad superior cuando los hechos hubieran sido cometidos por el cónyuge o por persona que esté o haya estado unida a él por análoga relación de afectividad, aun sin convivencia, la víctima fuera menor de edad o una persona con discapacidad necesitada de especial protección, o los hechos se hubieran cometido con una finalidad lucrativa".

[288] PALAZZI, Pablo. (2017). Consideraciones sobre la aprobación por el Senado de un proyecto de ley para penalizar la publicación de imágenes íntimas (revenge porn). El Derecho 19 de abril de 2017.

[289] DEMTSCHENKO, Marina, ZERDÁ, María Florencia (2018), "Violencia de Género Digital", Revista Jurídica, Género y Derechos, Abeledo Perrot

Para las autoras la respuesta es sí, si los cuerpos de las mujeres son objetivados y juzgados desde los albores de la humanidad, ¿por qué no lo serían en cada nuevo entramado social que surge?. Adhieren a la postura de la necesidad de llevar a cabo políticas públicas y, dentro de ellas, principalmente esfuerzos legislativos para identificar y penar los ciberabusos, sumando una concientización sobre el uso responsable y consciente de las nuevas tecnologías y redes sociales, todo ello con la correspondiente perspectiva de género, para evitar la proliferación de nuevas formas de violencia contra la mujer.

Coincidimos plenamente con estas autoras (y otras tantas que se encargan de visibilizar) que detrás de la comisión de este tipo de delitos (sobre todo el de difusión no consentida de material íntimo), estamos ante nuevas formas de ejercer violencia de género.

El fundamento de penalización de la conducta analizada bien podría encontrarse en la Convención Interamericana para prevenir, sancionar y erradicar la violencia contra la mujer (conocida como "Convención de Belem do Pará"), ratificada en Argentina por la Ley 24.632.

A modo de conclusión, si bien en Argentina ninguna de las propuestas citadas ha sido aprobada hasta el momento de escribir estas líneas, queda de manifiesto el interés que existe sobre esta figura, y su importancia en la consideración de las “nuevas figuras” relacionadas a ciberdelitos.

País	Delito 11: Violación de Datos Personales
Argentina	**Parcialmente aplicable. Ley 26.388 - Artículo 157 bis:** Será reprimido con la pena de prisión de un (1) mes a dos (2) años el que: 1. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales; 2. Ilegítimamente proporcionare o revelare a otro información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley. 3. Ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales. **Parcialmente aplicable. Artículo 155 CP:** Será reprimido con multa de pesos un mil quinientos ($ 1.500) a pesos cien mil ($ 100.000), el

País	Delito 11: Violación de Datos Personales
	que hallándose en posesión de una correspondencia, una comunicación electrónica, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, no destinados a la publicidad, los hiciere publicar indebidamente, si el hecho causare o pudiere causar perjuicios a terceros. Está exento de responsabilidad penal el que hubiere obrado con el propósito inequívoco de proteger un interés público.
Brasil	No se encontró tipificación.
Colombia	**CP Art. 269 F: Violación de datos personales.** El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.
México	**Parcialmente aplicable. CP. Art. 211 Bis.-** A quien revele, divulgue o utilice indebidamente o en perjuicio de otro, información o imágenes obtenidas en una intervención de comunicación privada, se le aplicarán sanciones de seis a doce años de prisión y de trescientos a seiscientos días multa **CP. Art. 199 Octies.-** Comete el delito de violación a la intimidad sexual, aquella persona que divulgue, comparta, distribuya o publique imágenes, videos o audios de contenido íntimo sexual de una persona que tenga la mayoría de edad, sin su consentimiento, su aprobación o su autorización. Así como quien videograbe, audiograbe, fotografíe, imprima o elabore, imágenes, audios o videos con contenido íntimo sexual de una persona sin su consentimiento, sin su aprobación, o sin su autorización. Estas conductas se sancionarán con una pena de tres a seis años de prisión y una multa de quinientas a mil Unidades de Medida y Actualización.
España	**CP Art. 197**. 1. El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales, intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses. 2. Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio

País	Delito 11: Violación de Datos Personales
	del titular de los datos o de un tercero. 3. Se impondrá la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores. Será castigado con las penas de prisión de uno a tres años y multa de doce a veinticuatro meses, el que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realizare la conducta descrita en el párrafo anterior. 4. Los hechos descritos en los apartados 1 y 2 de este artículo serán castigados con una pena de prisión de tres a cinco años cuando: a) Se cometan por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros; o b) se lleven a cabo mediante la utilización no autorizada de datos personales de la víctima. Si los datos reservados se hubieran difundido, cedido o revelado a terceros, se impondrán las penas en su mitad superior. 5. Igualmente, cuando los hechos descritos en los apartados anteriores afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere un menor de edad o una persona con discapacidad necesitada de especial protección, se impondrán las penas previstas en su mitad superior. 6. Si los hechos se realizan con fines lucrativos, se impondrán las penas respectivamente previstas en los apartados 1 al 4 de este artículo en su mitad superior. Si además afectan a datos de los mencionados en el apartado anterior, la pena a imponer será la de prisión de cuatro a siete años. 7. Será castigado con una pena de prisión de tres meses a un año o multa de seis a doce meses el que, sin autorización de la persona afectada, difunda, revele o ceda a terceros imágenes o grabaciones audiovisuales de aquélla que hubiera obtenido con su anuencia en un domicilio o en cualquier otro lugar fuera del alcance de la mirada de terceros, cuando la divulgación menoscabe gravemente la intimidad personal de esa persona. Se impondrá la pena de multa de uno a tres meses a quien habiendo recibido las imágenes o grabaciones audiovisuales a las que se refiere el párrafo anterior las difunda, revele o ceda a terceros sin el consentimiento de la persona afectada. En los supuestos de los párrafos anteriores, la pena se impondrá en su mitad superior cuando los hechos hubieran sido cometidos por el cónyuge o por persona que esté o haya estado unida a él por análoga relación de afectividad, aun sin convivencia, la víctima fuera menor de edad o una persona con discapacidad necesitada de especial protección, o los hechos se hubieran cometido con una finalidad lucrativa

Tabla Nº 14: Cuadro comparativo de tipificación de Delito 11: Violación de Datos Personales

4.7. Generación de estadísticas

A partir de aquí, resumimos los resultados alcanzados con la construcción de estadísticas calculadas a partir de los resultados obtenidos en el estudio de derecho comparado.

Recordamos que en los casos donde consideramos que la figura penal estudiada no se encuentra tipificada en su totalidad, pero existen otras figuras penales que podrían ser aplicadas a partes de esas conductas, se ha optado por señalarlos en las tablas como **"parcialmente aplicables"**

País	1. Acceso Ilícito	2. Interceptación Ilícita	3. Atentado contra la integridad de los datos	4. Atentado contra la Integridad del sistema	5. Abuso de los dispositivos
Argentina	Art. 153 bis	Art. 153	Art. 183 2do p.	Art. 183 2do p. Art. 197	Art. 183 2do p.
Brasil	Art. 154-A	Art. 56 Ley Nº 9296 Art. 10	Art. 154-A	Art. 266	No se encontraron tipos penales aplicables
Colombia	Art. 269 A	Art. 269 C	Art. 269 D	Art. 269 B	Art. 269 E Art. 269 F Art. 269 G
México	Art. 211 bis 1	Art. 168 bis	Art. 211 bis 2	Art. 211 bis 2, 3, 4 y 5	Art. 168 ter Art. 424 bis
España	Art. 197 bis	Art. 197 2do párr.	Art. 264	Art. 264 bis	Art. 197 ter

País	6. Falsedad Informática	7. Fraude o Estafa Informática	8. Relacionados con Abuso Sexual Infantil	9. Suplantación de Identidad Digital	10. Captación ilegítima de datos	11. Violación de Datos Personales
Argentina	Art. 292 Art. 183 2do p.	Art. 172 Art. 173 inc. 16	Art. 128	CABA - Art. 68 q.	Art. 157 bis	Art. 157 bis Art. 155
Brasil	Art. 298	Art. 155 4º B	Art. 241-A Art. 241-B	No se encontraron tipos penales aplicables	No se encontraron tipos penales aplicables	No se encontraron tipos penales aplicables

Colombia	Art. 269 D Art. 269 G	Art. 269 J	Art. 218	Art. 296	Art. 269 G	Art. 269 F
México	Art. 211 bis 3, 4 y 5	Art. 386	Art. 202 Art. 202 bis	No se encontraron tipos penales aplicables	No se encontraron tipos penales aplicables	Art. 211 bis Art. 199 Oct
España	Art. 399 bis y ter Art. 249	Art. 248 y 249	Art. 189	Art. 401	Art. 249	Art. 197

Tabla Nº 15: Cuadro Resumen de Derecho Comparado sobre Delitos Informáticos

4.8.1. Regulación de delitos por países

El primero de los datos que es posible obtener, es sobre el nivel de regulación de los delitos informáticos de cada uno de los países. Por ello, se ha procedido a realizar un análisis cuantitativo sobre la cantidad de delitos informáticos que cada país tiene regulado, los cuáles en primera instancia son publicados con el orden de los países en los cuáles el estudio ha sido abordado.

Adicionalmente, separamos en un primer cuadro (a), la segmentación de los delitos informáticos (1 a 8), que son aquellas sugeridos por los instrumentos internacionales (y de interés para nuestra hipótesis de trabajo) y luego, en un segundo cuadro (b) más completo, la totalidad (11) de los delitos informáticos incluídos en el estudio.

País	Delitos tipificados	Delitos parcialmente tipificados	Delitos No Tipificados	Total
Argentina	75,00%	25,00%	0,00%	100,00%
Brasil	75,00%	25,00%	0,00%	100,00%
Colombia	87,50%	12,50%	0,00%	100,00%
México	75,00%	25,00%	0,00%	100,00%

España	87,50%	12,50%	0,00%	100,00%

Tabla Nº 16a: Cuadro comparativo de estadísticas de tipificación en Delitos Informáticos sugeridos internacionalmente (ordenados alfabéticamente)

País	Delitos tipificados	Delitos parcialmente tipificados	Delitos No Tipificados	Total
Argentina	54,55%	45,45%	0,00%	100,00%
Brasil	54,55%	18,18%	27,27%	100,00%
Colombia	81,82%	18,18%	0,00%	100,00%
México	63,64%	18,18%	18,18%	100,00%
España	81,82%	18,18%	0,00%	100,00%

Tabla Nº 16b: Cuadro comparativo de estadísticas de tipificación en Delitos Informáticos (ordenados alfabéticamente)

En un segundo cuadro, estos mismos resultados han sido ordenados numéricamente generando una especie de "*ranking*" de los países que mayor regulación penal poseen al respecto.

Nuevamente, separamos en un primer cuadro (a), la segmentación de tipos penales (de 1 a 8), que son aquellos sugeridos por los instrumentos internacionales (y de interés para nuestra hipótesis de trabajo) y luego, en un segundo cuadro (b) más completo, la totalidad (11) de los tipos penales considerados en el estudio.

Ranking	País	Delitos tipificados	Delitos parcialmente tipificados	Delitos No Tipificados	Total
1	Colombia	87,50%	12,50%	0,00%	100,00%
2	España	87,50%	12,50%	0,00%	100,00%
3	Argentina	75,00%	25,00%	0,00%	100,00%
4	México	75,00%	25,00%	0,00%	100,00%

5	Brasil	75,00%	25,00%	0,00%	100,00%

Tabla Nº 17a: Ranking de estadísticas de tipificación en Delitos Informáticos sugeridos internacionalmente (ordenados por países con mayor nivel de cumplimiento)

Ranking	País	Delitos tipificados	Delitos parcialmente tipificados	Delitos No Tipificados	Total
1	Colombia	81,82%	18,18%	0,00%	100,00%
2	España	81,82%	18,18%	0,00%	100,00%
3	Argentina	54,55%	45,45%	0,00%	100,00%
4	México	63,64%	18,18%	18,18%	100,00%
5	Brasil	54,55%	18,18%	27,27%	100,00%

Tabla Nº 17b: Ranking de estadísticas de tipificación en Delitos Informáticos (ordenados por países con mayor nivel de cumplimiento)

4.8.2. Nivel de tipificación por delito

Como segundo dato de importancia que es posible obtener a partir de este estudio, consiste en analizar el nivel de regulación penal en todos los países alcanzados, de acuerdo a cada una de las figuras penales estudiadas.

De esta forma, podremos observar cuales son los delitos informáticos con mayor recepción y cuáles son aquellos que menor consenso tiene a nivel jurídico.

Id.	Delito tipificado	Tipificado	Parcialmente tipificado	No Tipificado
1	Acceso ilícito a sistemas o datos informáticos (intrusismo informático)	100,00%	0,00%	0,00%
2	Interceptación ilícita de sistemas o datos informáticos	100,00%	0,00%	0,00%

3	Ataques a la integridad de datos informáticos (cracking)	100,00%	0,00%	0,00%
4	Ataques a la integridad de sistemas informáticos (denegación de servicios)	100,00%	0,00%	0,00%
5	Abuso de dispositivos	40,00%	60,00%	0,00%
6	Falsificación informática	00,00%	100,00%	00,00%
7	Fraude informático	100,00%	00,00%	00,00%
8	Delitos relacionados con el abuso sexual infantil	100,00%	0,00%	0,00%
9	Suplantación de identidad digital	00,00%	60,00%	40,00%
10	Captación ilegítima de datos confidenciales (phishing)	40,00%	20,00%	40,00%
11	Violación de datos personales	60,00%	20,00%	20,00%

Tabla Nº 18: Estadísticas que indican en porcentajes el nivel de regulación de cada delito informático en la totalidad de los países incluídos en el estudio (ordenados de acuerdo al orden del análisis)

Ranking	Id.	Delito tipificado	Tipificado	Parcialmente tipificado	No Tipificado
1	1	Acceso ilícito a sistemas o datos informáticos (intrusismo informático)	100,00%	0,00%	0,00%
2	2	Interceptación ilícita de sistemas o datos informáticos	100,00%	0,00%	0,00%
3	3	Ataques a la integridad de datos informáticos (cracking)	100,00%	0,00%	0,00%
4	4	Ataques a la integridad de sistemas informáticos (denegación de servicios)	100,00%	0,00%	0,00%
5	7	Fraude informático	100,00%	00,00%	00,00%
6	8	Delitos relacionados con el abuso sexual infantil	100,00%	0,00%	0,00%

7	11	Violación de datos personales	60,00%	20,00%	20,00%
8	5	Abuso de dispositivos	42,86%	42,86%	14,29%
9	9	Suplantación de identidad digital	38,10%	14,29%	47,62%
10	6	Falsificación informática	33,33%	28,57%	38,10%
11	10	Captación ilegítima de datos confidenciales (phishing)	14,29%	19,05%	66,67%

Tabla Nº 19: Estadísticas que indican en porcentajes el nivel de regulación de cada delito informático en la totalidad de los países incluídos en el estudio (ordenados por delitos con mayor nivel de tipicidad)

4.8. Análisis de los resultados obtenidos

Para comenzar, a nivel genérico normativo es posible afirmar que ninguno de los países incluídos en el alcance de esta tesis han optado por una regulación más integral en relación al cibercrimen. Es decir, de acuerdo a la "*Tabla Nº 1: Legislación vigente en materia de delitos informáticos en los países incluídos en el estudio*" podemos observar que los 5 países bajo estudio procedieron a realizar modificaciones o actualizaciones parciales de sus códigos penales vigentes, sin que esto implica la generación de una norma interna del estilo del Convenio de Cibercrimen de Budapest.

A modo de ejemplo, puede citarse la normativa vigente en República Dominicana (Ley Nº 53/2007) donde incorporan conceptos propios, principios, parte penal material, parte procesal penal, e incluso se han generado los organismos dedicados a su investigación y persecución. A modo de primer conclusión preliminar podemos afirmar entonces que todos los países alcanzados han optado por un desarrollo más básico, a través de modificaciones parciales a sus Códigos Penales vigentes, adaptando las figuras penales clásicas a fin de que sea posible su aplicación en los delitos informáticos o agregando nuevas en algunos casos.

No obstante y a modo de aclaración interpretativa de los resultados aquí expuestos, debe la persona lectora del presente trabajo considerar que el hecho de no haberse encontrado normativa especial regulada sobre los delitos informáticos en estos países, no implica necesariamente que todas las conductas disvaliosas realizadas a través de medios informáticos puedan realizarse en ese país, sin ningún tipo de sanción o consecuencia jurídica por parte del Estado. Por un lado, porque pueden existir sanciones de otro tipo que no impliquen normas penales. Por otro, porque las propias normas penales pueden no ser especiales, y aún así pueden seguir aplicándose al caso concreto.

Que, hemos confirmado que por cuestiones atinentes a cada país en particular, su cultura jurídica penal en cuanto a la forma de redacción de los tipos penales, así como los diferentes bienes jurídicos que se protegen a través de ellos, hacen que las redacciones sean en algunos casos sustancialmente diferentes (sección 4.6), incluso tratando de reprimir penalmente la misma conducta. Los argumentos de la presente afirmación, pueden observarse a través del análisis de las tablas de los 11 delitos analizados, donde en muchos de los casos al momento de identificar un tipo penal aplicable a la conducta investigada, se termina aplicando delitos tipificados de forma más genérica, que incluyen a la conducta de estudio.

Que, dentro de la misma línea que el punto anterior, dentro de aquellos países que han dado respuesta positiva a la decisión de avanzar sobre cierta regulación penal sobre las conductas investigadas, pueden observarse diferencias sobre los elementos esenciales para punir la conducta de estudio. A modo de ilustración, podemos citar el caso de los elementos necesarios para considerar la tipificación penal del acceso indebido, donde encontramos países que tienen diferentes exigencias (con o sin medidas de seguridad, con o sin perjuicio a terceros, etc). Por lo tanto, si bien en determinadas figuras pareciera existir cierta coordinación, lo cierto es que al mirar con mayor nivel de detalle las conductas delictivas penalizadas, dicha coordinación empieza a mostrar pequeñas diferencias, notando las diferencias de criterios y técnicas legislativas de los países del estudio.

Que, entendemos que tanto la técnica jurídica, así como la elección de la pena para conducta (aspecto que no es tenido en cuenta al momento comparativo), responde a aspectos propios de cada uno de los Estados, de forma que no sería

pertinente realizar desde aquí apreciaciones que implicaría un desarrollo que excedería lo propuesto en los objetivos de la presente tesis.

Que, como hemos sostenido anteriormente, a fines de intentar adaptar cada tipo penal dentro de algunas de las categorías propuestas, ha sido necesario realizar un importante trabajo de interpretación, donde definitivamente se ha utilizado un criterio de interpretación amplio. Es decir, siempre que la figura penal conserve los elementos esenciales o básicos de la conducta delictiva en sí -no contemplando las características secundarias o adicionales propias de cada código o sistema penal-, se ha considerado dicha situación como "positiva", en el sentido de confirmar la existencia de una figura penal aplicable al delito categorizado.

Que, nos parece de interés académico hacer referencia que se ha detectado en el análisis de las distintas conductas (sección 4.6) que en varios casos existen tipos penales que incluyen más de un delito en su interior. Por esa razón, pueden encontrarse casos donde para distintos delitos, la figura penal es la misma. Por ejemplo, pasa en el caso de Argentina, en relación a la tipificación de la figura de acceso ilícito e interceptación ilícita, ambos comportamientos penados por la misma figura penal (183 del CP).

4.9. Conclusiones sobre el nivel de tipificación de los delitos informáticos alcanzados

Que, de acuerdo a los resultados exhibidos en la Tabla Nº 17 Ranking de estadísticas de tipificación en Delitos Informáticos, se puede observar que de los países alcanzados, Colombia y España comparten el primer lugar en relación a su situación de tipificación de delitos informáticos, con un 81,82% de los delitos tipificados, y un 18,18% de delitos parcialmente tipificados.

Argentina presenta el tercer lugar con un 54,55% de delitos tipificados y un 45,45% de delitos parcialmente tipificados. México, ha quedado en 4º lugar ya que si bien en principio tiene un mayor nivel que Argentina en delitos tipificados (un 64,5

%), la realidad es que presenta un 18,18% de delitos parcialmente tipificados y un 18,18% de delitos no tipificados.

Es decir, considerando una interpretación global, Argentina posee algún tipo de sanción penal - en mayor o menor medida- para todos los delitos informáticos alcanzados en el estudio. En cambio, México presenta un 18,18% de los delitos sin ningún tipo de sanción penal (al menos no encontrada en el marco de la presente investigación). En último lugar ha quedado Brasil, con un 54,55% de las conductas tipificadas (igual que Argentina), un 18,18% de las conductas parcialmente tipificadas y un 27,27% de delitos no tipificados, alcanzando el mayor nivel de falta de tipificación dentro de los países estudiados.

A nivel general podemos afirmar entonces que, de la totalidad de delitos seleccionados para formar parte de este estudio, los que estadísticamente se encuentran más regulados, coinciden con aquellos que la Convención de Cibercrimen de Budapest considera como obligatorios para los Estados adheridos. De la Tabla Nº 19 puede observarse que los primeros seis delitos con mayor nivel de tipicidad, son precisamente aquellos pertenecientes al listado propuesto por dicho Convenio.

No obstante, dejamos constancia que para algunos delitos puntuales, como el caso de la falsificación informática (art. 7 del Convenio de Budapest), se ha encontrado un bajo nivel de regulación (está en el penúltimo puesto de todos los delitos investigados). Lo mismo con el delito de abuso de dispositivos (art. 6 del Convenio de Budapest) que en el ranking de los delitos más tipificados, se encuentra en el 8vo lugar, incluso después del delito de violación de datos personales, un delito que no está propuesto por Budapest.

Que, las explicaciones para ambas situaciones entendemos que pueden deberse a diversos motivos. Por un lado y en relación a la falsedad informática, no se han encontrado tipos penales exclusivamente dedicados a esta conducta, ya que en la mayoría de los países de estudio, se consideró como parcialmente aplicable la falsificación de documentos (entendiendo que el concepto documento incluye al dato informático).

En segundo lugar y en relación al delito de abuso de dispositivos, entendemos que la propuesta de dicha conducta representa un adelantamiento de la barrera

penal, ya que considera la tipificación de conductas como la tenencia o producción de sistemas o dispositivos destinados a la comisión de alguno de los delitos informáticos, aspectos que depende mucho de la postura de cada país en relación al expansionismo penal (analizado en la sección 2.8) de la presente tesis.

Que, considerando los datos resultantes de los delitos informáticos que hemos agregado por fuera del Convenio de Budapest, -suplantación de identidad digital, captación ilegítima de datos confidenciales, violación de datos personales-, los resultados sobre el nivel de regulación penal puede llegar a verse más desalentadores, toda vez que como puede observarse, salvo excepciones, la mayoría de los países poseen un bajo nivel de regulación, estando por debajo del 60%.

Capítulo V: La afectación de derechos a través de medidas de injerencia

5.1. Introducción

La delincuencia evoluciona. Los delincuentes cada vez se organizan mejor, cada vez se sienten más seguros utilizando las nuevas -o ya no tan nuevas- tecnologías de la información y las comunicaciones. Los delincuentes ya no se llaman por teléfono para organizarse sobre el nuevo comercio que piensan atracar, sino que ahora se escriben por Whatsapp, o peor aún, se llaman por Whatsapp. Algunas bandas ya utilizan Telegram o Signal para estar comunicados. Los delincuentes relacionados al comercio y distribución de pornografía infantil, envían contenidos a través de proxys anónimos y usan contenedores virtuales cifrados para almacenar su colección privada.

La delincuencia se complejiza, se expande y continúa evolucionando. Las preguntas, pensando en el otro lado del mostrador y que motiva la generación de este capítulo es: ¿La justicia también evolucionó lo suficiente para estar preparados para la detección, identificación y captura de los ciberdelincuentes? ¿Los métodos de investigación utilizados por el Estado, responden a estas nuevas realidades de la delincuencia? y por último y quizás más importante ¿Cuál es el nivel de afectación de los derechos en la utilización de estos nuevos métodos de investigación?

La persecución y condena de los delitos informáticos depende de un factor clave: conseguir la evidencia digital necesaria para poder probar ante el juez competente, la culpabilidad de una o más personas en su participación en dichos hechos delictivos.

Si bien el acceso a la evidencia digital puede darse de diversas formas, es muy probable que en el marco de la mayor parte de las investigaciones penales (en

su etapa preparatoria) sea necesario acudir a una serie de medidas de investigación que tengan por finalidad la obtención de dicha evidencia.

Partimos de la base que las investigaciones sobre delitos cibernéticos que llevan adelante las fiscalías y fuerzas de seguridad, requieren de una variada gama de técnicas de investigación adecuadas para esta forma delictiva.

Aunque en determinadas ocasiones se pueden lograr algunas acciones investigativas con las facultades tradicionales (por ejemplo, llevar adelante un allanamiento puede ser necesario en muchos casos), no quedan dudas de la necesidad respecto la regulación de herramientas procesales específicas para estos casos.

Alertamos al lector que somos conscientes que el abordar el tema de evidencia digital, así como de medidas de investigación en general es un tema demasiado complejo y profundo, que excede el alcance de la presente tesis.

No obstante, considerando y entendiendo la necesidad de comprobación de la hipótesis planteada en este trabajo, comenzaremos el capítulo con la finalidad de generar un mínimo marco teórico sobre estos temas, destacando la problemática observada y sentando nuestro punto de vista al respecto.

Una vez resueltas dichas bases, si avanzaremos a dar cumplimiento a una de las metas propuestas en esta tesis: identificar la existencia de medidas de investigación reguladas que tengan por destino la persecución de los delitos informáticos (previa elección de los medidas de investigación alcanzadas) en los distintos ordenamientos jurídicos incluídos en el estudio y compararlas con los instrumentos internacionales de lucha contra el cibercrimen.

5.2. Indicios y Evidencia

El campo principal de la labor de las diversas disciplinas forenses es el de la búsqueda, análisis y/o interpretación de evidencia. Aunque en Criminalística, los

términos evidencia e indicio funcionan como sinónimos, es conveniente utilizar sólo el primero de ellos.

Las ciencias forenses consideran evidencia o indicio a todo objeto, marca, huella, señal, vestigio, es decir, todo aquello que deja la realización de un delito como testigo de haber acontecido.

Para la Criminalística[290], indicio es toda evidencia física que tiene estrecha relación con la comisión de un hecho presuntamente delictuoso, cuyo examen o estudio proporciona las bases científicas para encaminar con buenos principios la investigación y lograr fundamentalmente:

a) la identificación del o los autores,

b) las pruebas de la comisión del hecho y

c) la reconstrucción del mecanismo del hecho.

Edmond Locard se refería a los indicios como los testigos mudos que no mienten[291]. La denominada prueba indiciaria posee tres elementos: un hecho comprobado (hecho indicador, de carácter contingente), una operación lógica o juicio de razonamiento y, como fruto de este razonamiento, un hecho indicado (aquél que se pretende probar y forma parte del objeto de la controversia). En el marco procesal, una evidencia requiere su adecuada presentación y/o análisis para transformarse en fuente de indicios. Son los testigos y los expertos (y posteriormente los litigantes en sus alegatos) quienes hacen “hablar” a las evidencias, dotándolas de un valor indiciario más o menos convincente[292].

Desde el punto de vista procesal, las evidencias pueden cumplir esencialmente dos funciones[293]:

---

[290] MONTIEL SOSA, J. (2003) Manual de Criminalistica. Ed. Limusa. Grupo Noriega Editores. México D.F. p.49.
[291] MORENO GONZALEZ, L. (1977) Manual de introducción a la Criminalística. Ed. Porrúa, S. A. México.
[292] GARCÍA CAVERO, P. (2019). El valor probatorio de la prueba por indicios en el nuevo proceso penal. Revista De Derecho, 11(1), 53–69. Recuperado a partir de https://revistas.udep.edu.pe/derecho/article/view/1528
[293] DI IORIO, Ana Haydée …, “El rastro digital del delito : aspectos técnicos, legales y estratégicos de la informática forense”,1a ed . - Mar del Plata : Universidad FASTA, 2017

Función orientadora: la evidencia proporciona una pista o hilo conductor que permite avanzar en una investigación. La pista por sí misma no necesariamente acredita un extremo del hecho investigado. Un ejemplo de ello es la obtención de una dirección IP que conduzca luego a un domicilio físico.

Función probatoria: la evidencia puede ser invocada como prueba de los hechos que afirma una de las partes del proceso. Por ejemplo: un archivo de video que aparece captando una colisión vehicular o un intento de cohecho.

Una evidencia puede cumplir sucesivamente ambas funciones. Es relevante recordar que cuando se pretende emplear evidencia en función probatoria, deben haberse cumplido los requisitos de relevancia, suficiencia, confiabilidad y validez de esa prueba.

En este marco cabe decir que la incorporación de las tecnologías de información a la vida cotidiana ha marcado la necesidad de incluir a los medios informáticos como elementos de carácter investigativo y/o probatorio, y, a su vez, la obtención, examinación, análisis, interpretación y presentación de esta clase de evidencia, ha requerido el auxilio de expertos en la temática.

Siguiendo a Michelle Taruffo[294], cabe distinguir dos concepciones de la prueba: como instrumento de conocimiento y como instrumento de persuasión . La primera noción de prueba, como elemento cognoscitivo, la concibe como el conjunto de elementos, procedimientos y razonamientos mediante los cuales se busca y se establece la verdad de los hechos.

Desde esta perspectiva, la prueba ofrece informaciones relativas a los hechos que deben ser determinados en el proceso, permitiendo su reconstrucción, confirmada y verificada como verdadera, precisamente a través de la actividad probatoria. De acuerdo con la segunda concepción, la prueba sería un instrumento de persuasión, que no serviría para establecer la verdad o falsedad de enunciado

[294] TARUFFO, Michele, "Algunas consideraciones sobre la relación entre prueba y verdad", en La prueba. Artículos y conferencias (Santiago: Metropolitana 2008), 59-66, https://letrujil.files.wordpress.com/2012/01/la-prueba-michele-taruffo.pdf

alguno, sino para persuadir al juez, esto es, para convencerlo de lo fundado o infundado de un enunciado fáctico[295] .

Ahora bien, este entendimiento legal de la prueba no debería conducir, en una interpretación literal del precepto, a desatender la función de la prueba como herramienta para conocer y verificar los hechos. Y ello porque, aunque el aspecto argumentativo y persuasivo no puede considerarse totalmente ajeno a la prueba, si se admite que esta no sirve para determinar la verdad o falsedad de los enunciados o para conocer los hechos, sino tan solo para persuadir al juez, se estaría admitiendo, en definitiva, que el conocimiento de la verdad es un fin ajeno al proceso. En este sentido, una vez más, las palabras de Taruffo resultan esclarecedoras e inspiradoras: "Sería, por decir lo menos, paradójico que, en un sistema democrático, inspirado en el valor de la verdad, la administración de justicia no se inspirara, sin embargo, en ese valor o, más aún, se fundara sistemáticamente en el error, en la mentira y en la distorsión de la verdad"[296].

5.3. Principios probatorios

Consideramos de importancia para el desarrollo del presente trabajo, formando parte del marco teórico en esta sección dedicada al Derecho Procesal Penal, tener al menos un breve desarrollo de los principios probatorios más importantes a nivel general, con la finalidad de luego poder hacer referencia a los más importantes para el ámbito de la evidencia digital.

Desarrollaremos aquellos principios relativos al momento adecuado para proponer y practicar las pruebas, aquellos que informan la decisión de admisión o inadmisión de las pruebas propuestas y, así mismo, aquellos principios que han de informar la práctica o producción de pruebas ante el juzgador.

[295] Sobre estas y otras funciones de la prueba, véase Michele Taruffo, La prueba de los hechos (Madrid: Trotta, 2002), 80-89

[296] TARUFFO, Michelle: "Simplemente la verdad: el juez y la construcción de los hechos"; Madrid: Marcial Pons, 2010, Pág. 115.

Muchos de los principios que se referencian y se definen aquí se encuentran interrelacionados entre sí. Así, por ejemplo, los principios de igualdad de oportunidades y de contradicción, que, aunque tienen un contenido autónomo, son complementarios entre sí.

Los principios enumerados en este precepto podrían clasificarse en tres categorías.

1) Principios del proceso, donde se ubicaran los principios estructurales del proceso, que informan, en este caso, la actuación de las partes en cuanto a la actividad probatoria (principios de contradicción e igualdad de oportunidades).

2) Principios del procedimiento, relativos a la forma y momento en que han de producirse los actos de prueba (principios de pertinencia e inmediación).

3) Principios relativos a la admisibilidad de las pruebas, que vienen a determinar los medios de prueba admisibles en abstracto (principio de libertad probatoria), así como los criterios para determinar su admisibilidad en el caso concreto (principio de exclusión y principio de pertinencia).

5.3.1. Principio de oportunidad

El principio de oportunidad se refiere al momento procesal oportuno para proponer y practicar la prueba. El momento para proponer la prueba es la etapa de evaluación y preparatoria de juicio, por lo tanto, siempre de forma previa a la audiencia oral del juicio, con lo que se viene a garantizar la debida contradicción, en tanto que principio estructural del proceso y derecho fundamental de las partes.

Por otra parte, la determinación legal del momento oportuno para proponer la prueba se relaciona con el principio de preclusión procesal, de tal forma que, transcurrida la etapa procedimental prevista para tal actividad propositiva, las partes perderán la posibilidad de proponer pruebas posteriormente.

Con el principio de oportunidad y su complementario, el de preclusión, se busca, por una parte, garantizar que las partes conozcan oportunamente las pruebas

propuestas de contrario y, por otra, que el proceso no sufra dilaciones indebidas provocadas por la presentación de pruebas extemporáneas.

Así mismo, con esta ordenación de la actividad probatoria se garantizan otro de los principios estructurales que ha de informar el proceso en general, y la actividad probatoria en particular, el principio de igualdad de oportunidades. Por otra parte, el precepto fija como momento oportuno para la práctica de la prueba la audiencia del juicio, lo cual constituye garantía de inmediación y posibilita la oralidad, como principio del procedimiento que también ha de informar la actividad probatoria.

El hecho de que las pruebas en que se base el juzgador sean exclusivamente aquellas practicadas en el juicio oral, como reconoce este precepto, fue seguramente uno de los mayores logros de la Ley de Enjuiciamiento Criminal española de 1882, cuya magistral exposición de Motivos se refiere a "la idea fundamental de que en el juicio oral y público es donde ha de desarrollarse con amplitud la prueba, donde las partes deben hacer valer en igualdad de condiciones los elementos de cargo y descargo, y donde los Magistrados han de formar su convicción para pronunciar su veredicto con abstracción de la parte del sumario susceptible de ser reproducida en el juicio" como una de las principales ideas inspiradores de un proceso penal moderno y de naturaleza acusatoria, frente al antiguo modelo inquisitivo, en el que el mismo juez que conducía la investigación, valoraba las pruebas y dictaba sentencia.

Siguiendo este modelo, las únicas pruebas a tomar en consideración en la sentencia serán las practicadas en la audiencia oral del juicio, señalando que las actuaciones realizadas durante la fase de investigación sólo alcanzarán valor probatorio cuando sea incorporadas al juicio oral, a través de su práctica ante el tribunal sentenciador, con sujeción a los principios de inmediación, contradicción e igualdad.

5.3.2. Principio de inmediación

Históricamente, la inmediación irrumpe como principio básico del procedimiento en tanto que implicación necesaria del proceso oral y público[297].

Para Calamandrei[298], "inmediación significa presencia simultánea de los varios sujetos del proceso en el mismo lugar y, por consiguiente, posibilidad entre ellos de cambiarse oralmente sus comunicaciones".

La mayor parte de los autores, al estudiar el principio de inmediación se centran en la relación del juez con las fuentes de prueba. En este sentido, el principio de inmediación exige que el órgano que va a dictar la sentencia sea el que presencie directamente la práctica de las pruebas, examinando personalmente los documentos y escuchando tanto a las partes como a los testigos y peritos llamados a comparecer en la audiencia de juicio sin intermediarios ni interferencias[299].

Este principio supone, en definitiva, que el juez sentenciador ha de percibir por sus propios sentidos la práctica de la prueba en que basará su convicción. Se trata, por lo tanto, de garantizar la inmediatez entre los medios probatorios y el juzgador como garantía de una adecuada valoración de la prueba[300].

En sentido negativo, la garantía de inmediación supone la exclusión de cualquier tipo de intermediación entre el juez y las fuentes de pruebas, especialmente en el caso de las pruebas personales. De esta forma, se evita que sean tomadas en consideración en la decisión judicial pruebas practicadas fuera del acto de audiencia oral, especialmente sin la participación del juez sentenciador, como podrían ser los testimonios prestados ante la Fiscalía u otros órganos encargados de la investigación penal[301]. Y ello porque, en palabras de Pagano, "en

---

[297] PERFECTO, Andrés Ibáñez, "Sobre el valor de la inmediación. Una aproximación crítica", Jueces para la democracia, nº 26 (2003), 57-66, 57.
[298] CALAMANDREI, Piero; Instituciones de Derecho Procesal Civil, I, trad. Sentís Melendo (Buenos Aires: Ejea, 1973), 330
[299] PERFECTO, Andrés Ibáñez, "Sobre el valor de la inmediación. Una aproximación crítica", Jueces para la democracia, nº 26 (2003), 57-66, 57
[300] Según la STC 142/2012, de 2 de julio, los principios de publicidad, oralidad, inmediación y contradicción deben de rodear el conocimiento de la actividad probatoria para la adecuada valoración de las pruebas (F. J. 5º).
[301] TORRES, William, "Oralidad-inmediación-concentración", Derecho Penal y Criminología 24, nº. 74 (2003), 183-194, esp. 186-187.

la viva voz hablan también el rostro, los ojos, el color, el movimiento, el tono de voz, el modo de decir, y tantas otras pequeñas circunstancias, que modifican y desarrollan el sentido de las palabras y suministran tantos indicios a favor o en contra de lo afirmado con ellas"[302].

5.3.3. Principio de contradicción

El principio de contradicción, junto con el de igualdad de armas u oportunidades, constituye un principio estructural y fundamental de todo proceso judicial[303].

Este principio debería de ser respetado a lo largo de todo el procedimiento, incluida la fase de instrucción, aunque en la fase de juicio oral y, señaladamente, en la práctica de la prueba, cobra una especial relevancia y vigor[304].

En sentido amplio, el principio de contradicción consiste en la efectiva posibilidad de que toda persona, que se halle expuesta a ser afectada en su posición jurídica por una resolución judicial, pueda influir en el contenido de la misma, mediante la adquisición de conocimiento de los materiales en que ha de fundarse, la toma de postura respecto a los mismos y la participación en la introducción en el proceso de materiales que le sean favorables[305].

En este entendimiento amplio del principio, cabe incidir en que la contradicción no implica únicamente respetar la posibilidad de las partes de ejercer el derecho a defender sus pretensiones al mismo tiempo que contradicen las pretensiones de la contraparte, sino también asegurar que las partes pueden participar en el

---

[302] PAGANO, Francesco Mario, "Considerazioni sul processo criminale" (Stamperia Raimondiana: Nápoles, 1794), 106.
[303] SENDRA, Vicente Gimen, Fundamentos del Derecho Procesal, (Madrid: Civitas, 1981), 183-187
[304] Según el Tribunal Constitucional español la contradicción se manifiesta en las distintas fases del proceso, constituyendo una regla esencial del desarrollo del mismo y una exigencia ineludible del derecho a un proceso con todas las garantías (SSTC 218/1997, de 4 de diciembre, 138/1999, de 22 de julio, y 91/2000), sin cuya concurrencia, la idea de juicio justo es una simple quimera (STC 91/2000, de 30 de marzo, FJ 14º).
[305] ORTELLS RAMOS, Manuel y ARMENGOT VILLAPLANA, Alicia; "Los principios del proceso (I)", en AA.VV. Ortells Ramos (Dir. y Coord.), Introducción al Derecho Procesal, 4ª ed. (Navarra: Aranzadi, 2014), 317- 348, esp. 319.

procedimiento con el fin de influir en su resultado, entendido así, el contradictorio, como mecanismo político-legal de control del poder jurisdiccional[306].

El principio de contradicción, aplicado a la actividad probatoria, implica la posibilidad de las partes de controvertir o contradecir las alegaciones realizadas y las pruebas propuestas por la parte contraria. Se entiende, por lo tanto, que es "un elemento nuclear de la actividad probatoria", que supone que "las pruebas que se incorporen al proceso deban ser conocidas por ambas partes, para poder ser objeto de debate, pudiendo, en su caso, plantear medios de prueba de contrario"[307].

El respeto debido a este principio permite que los elementos de convicción en que se base el juzgador para decidir la causa, pasen por el tamiz de ambas partes, de forma que los aportados por una puedan ser refutados por la otra antes de que el juez tome posición respecto de los mismos, a través de la actividad de valoración probatoria. Condición para que la contradicción sea real, es el oportuno conocimiento de la prueba por las partes. En este sentido, la contradicción, en tanto que principio estructural del proceso, presupone, por supuesto, la dualidad de partes, así como el previo conocimiento de la acusación para poder ejercer la defensa.

En este sentido, el anuncio por las partes de las pruebas de las que intenten valerse en la fase preparatoria del juicio constituye requisito esencial para el oportuno conocimiento de las pruebas por la contraparte, siendo tal conocimiento, a su vez, presupuesto de una efectiva contradicción.

La posibilidad de contraste y refutación en qué consiste el principio de contradicción se erige, además, en garantía del eficaz acercamiento a la verdad. En este sentido, tal y como afirma Ferrajoli[308]: "*la verdad perseguida por el modelo acusatorio, concebida como verdad relativa o forma, se adquiere, como en cualquier*

[306] ZUFELATO, Camilo, "La dimensión de la «prohibición de la decisión-sorpresa» a partir del principio de contradicción en la experiencia brasileña y el nuevo Código Procesal Civil de 2015: reflexiones de cara al derecho peruano", Derecho PUCP: Revista de la Facultad de Derecho, nº 78 (2017): 21-42, esp. 23.
[307] BARONA VILAR, Silvia, "Objeto de la prueba y principios esenciales de la actividad probatoria", en AA.VV. Mª Isabel González Cano (Dir.); Mª Isabel Romero Pradas (coord.) La prueba. Tomo II. La prueba en el proceso penal, (Valencia: Tirant Lo Blanch, 2017), 77-148, esp. 16
[308] FERRAJOLI, Luigi; Derecho y Razón. Teoría del garantismo penal (Madrid: Editorial Trotta, 1995), 610.

investigación empírica, a través del procedimiento por ensayo y error. La principal garantía de su obtención se confía a la máxima exposición de las hipótesis acusatorias a la refutación de la defensa, es decir, al libre desarrollo del conflicto entre las dos partes del proceso, portadores de puntos de vista contrastantes, precisamente porque son titulares de intereses opuestos".

5.3.4. Principio de libertad probatoria

El principio de libertad probatoria consagra, en realidad, el principio de libertad de medios de prueba, indicando que todos los medios probatorios son válidos, sin que exista una lista tasada o cerrada de vías por las cuales las fuentes de prueba puedan acceder al proceso.

Ello es así, en primer lugar, porque el juicio de admisibilidad de las pruebas depende, normalmente, de su utilidad para la determinación de los hechos, y no de la existencia de una norma expresa que le dé amparo[309]. Y, en segundo lugar, porque, normalmente, las fuentes de prueba atípicas pueden ser introducidas en el proceso a través de su reconducción a alguno de los medios de prueba análogos regulados en la norma.

En cualquier caso, de acuerdo con este precepto, la única limitación al acceso de las fuentes de prueba al proceso se encontraría en los requisitos de pertinencia y de legalidad, que son, en definitiva, los criterios de admisibilidad de las pruebas. Por lo tanto, de acuerdo con este apartado, se admitirá cualquier medio de prueba pertinente, en tanto que, referido a hechos o circunstancias relevantes para el enjuiciamiento, y legal, esto es, no contrario a "la Constitución, los instrumentos internacionales de derechos humanos, los instrumentos internacionales ratificados por el Estado y demás normas jurídicas".

En definitiva, el principio de libertad probatoria supone que debe de permitirse la incorporación de todos aquellos elementos probatorios que contengan información relevante para el establecimiento de los hechos, a menos que existan normas legales expresas que los excluyan o condicionen.

[309] TARUFFO, Michelle; "La prueba de los hechos", Pág. 406

En palabras de Taruffo, "*cualquier prueba relevante debe de ser admitida, excepto que una norma jurídica específica la excluya o subordine su admisión a presupuestos o condiciones particulares*". De nuevo, se trata de un principio claramente preordenado a garantizar un eficaz acercamiento a la verdad, esto es, a maximizar las posibilidades de determinar de forma racional y aceptable los hechos, evitando al mismo tiempo la conducción de actividades procesales inútiles[310].

5.3.5. Principio de pertinencia

El principio de pertinencia implica que todas las pruebas propuestas, para ser admitidas, han de ser relevantes para acreditar hechos o circunstancias relativos a la infracción penal o a la responsabilidad del acusado.

Según Taruffo "la relevancia no es propiamente una cualidad de la prueba, sino característica constitutiva de la misma, en el sentido de que solo lo que es relevante puede ser definido como 'prueba' en un proceso"[311].

Muchas veces los códigos procesales con la finalidad de tender hacia el esclarecimiento de los hechos y la determinación de la verdad sea eficaz, indican expresamente que serán pertinentes, no solo las pruebas directamente referidas a los hechos relevantes, sino también las que indirectamente se refieren a la infracción penal y sus circunstancias o a la eventual responsabilidad del acusado.

Con esta distinción parece hacerse referencia a dos conceptos específicos propios del common law: *materiality* y *relevancy*. La primera cualidad, típica de la prueba directa, se refiere a la relevancia de los hechos jurídicos; mientras que, la segunda, se refiere a la prueba relativa a hechos secundarios, por lo tanto, no jurídicos, de los que pueden derivarse lógicamente consecuencias probatorias respecto del hecho principal[312].

---

[310] TARUFFO, Michelle; "La prueba de los hechos", Pág. 378
[311] TARUFFO, Michelle; "La prueba de los hechos", Pág. 365
[312] Sobre esta distinción entre prueba directa e indirecta, véase Michelle Taruffo, La prueba de los hechos, 365 y 453-460. De acuerdo con el autor, la distinción entre prueba directa o indirecta depende de la relación que se dé entre el hecho a probar y el objeto de la prueba. Por lo tanto, será prueba directa aquella que versa directamente sobre el hecho a probar. Y, en cambio, se estará ante una prueba indirecta cuando el objeto de la prueba esté constituido por un hecho distinto de aquel que debe de ser probado, pero que, a pesar de ello, resulta jurídicamente relevante a los efectos de la decisión.

En definitiva, como consecuencia de este principio, solo deben de admitirse aquellas pruebas relacionadas con los hechos que fundan la pretensión objeto del proceso, de las que pueda deducirse alguna consideración referente a la calificación jurídica del delito o que puedan servir para adquirir el convencimiento sobre la responsabilidad o irresponsabilidad del acusado[313].

5.3.6. Principio de exclusión

El principio de exclusión constituye la concreción legal de la norma constitucional según la cual las pruebas obtenidas o actuadas con violación de la Constitución o la ley no tendrán validez alguna y carecerán de eficacia probatoria.

El principio de exclusión es, al igual que el de pertinencia, una norma sobre la admisibilidad de las pruebas, en este caso, de contenido negativo o excluyente. En definitiva, especialmente en un sistema como el ecuatoriano, en el que rige la libertad de medios de prueba, si cualquier prueba relevante es en principio admisible[314], lo que determina este principio es una exclusión a posteriori de determinadas pruebas a la luz de ciertas normas jurídicas.

Concretamente, determina la inadmisibilidad y excluye, por lo tanto, la eficacia probatoria de aquellos elementos de convicción obtenidos en violación de los derechos reconocidos por la Constitución, por los tratados internacionales en materia de derechos humanos y, más generalmente, en la ley.

La amplitud con que se recoge esta norma de exclusión lleva a concluir que resultan inadmisibles las pruebas obtenidas vulnerando cualquier derecho que el ordenamiento jurídico reconozca.

---

[313] PEREZ CRUZ, Agustín, "La prueba y la presunción de inocencia en el Código Orgánico Integral Penal", Pág. 132.

[314] 9 Cabe referir, en este punto, la Rule 402 de las Federal Rules of Evidence norteamericanas, según la cual "*all relevant evidence is admissible*".

5.3.7. Principio de igualdad de oportunidades para la prueba

El principio de igualdad de oportunidades para la prueba constituye una concreción legal del derecho, consistente en presentar pruebas por la defensa y contradecir las que se presenten en su contra.

El derecho de presentar pruebas es concebido como garantía esencial del derecho de defensa. Ahora bien, tal y como se ha indicado en epígrafes anteriores, este derecho no es ilimitado, debiendo ser entendido como el derecho a utilizar las pruebas pertinentes para el proceso, no considerándose admisibles aquellas irrelevantes o impertinentes, así como las no permitidas por la ley y las presentadas fuera de plazo o sin respetar la legalidad procesal[315].

El principio de igualdad de armas se encuentra, así mismo, claramente conectado con el de contradicción. Igual que este, aquel debe de ser respetado en todas las fases procesales, y no exclusivamente en el marco del juicio oral, aunque sea en el momento de la práctica probatoria en el que cobra un vigor e importancia mayores.

Este principio implica que acusación y defensa han de contar con posibilidades análogas de actuación a lo largo del proceso, con idénticas oportunidades de alegar y probar lo que a su derecho convenga y, asimismo, de refutar las alegaciones y pruebas introducidas por la parte contraria. Tratándose de una garantía básica y estructural del debido proceso, cabe hacer hincapié en que corresponde a los órganos judiciales procurar que en el proceso se dé la necesaria contradicción entre las partes, así como que estas posean idénticas posibilidades de alegar o probar y, en definitiva, de ejercer su derecho de defensa en cada una de las instancias que lo componen[316].

---

[315] España Tribunal Constitucional, Sentencia 70/2002, de 3 de abril, Boletín Oficial del Estado 99, 25 de abril de 2002

[316] España Tribunal Constitucional, Sentencia 26/1988, de 28 de noviembre, Boletín Oficial del Estado 306, 22 de diciembre de 1988; España Tribunal Constitucional, Sentencia 162/1993, de 18 de mayo, Boletín Oficial del Estado 147, 21 de junio de 1993; o, España Tribunal Constitucional, Sentencia 154/2000, de 12 de junio, Boletín Oficial del Estado 165, 11 julio 2000

La igualdad formal se basa en que la ley no cree desigualdades en cuanto a las oportunidades de actuación de las partes y que no imponga a una de las partes una carga desproporcionada, atribuyéndole, por ejemplo, la carga de probar hechos negativos o su propia inocencia.

5.4. Evidencia digital en el proceso penal

Según Bielli y Ordoñez evidencia digital o evidencia electrónica es cualquier información probatoria almacenada o transmitida en formato digital, siendo que el material probatorio que surja de estas fuentes bien podrá ser usado por alguna de las partes que intervengan en el marco de un proceso judicial[317].

Siguiendo a estos mismos autores, la información electrónica se considera diferente de la evidencia originada en soporte papel debido a su forma intangible, volumen, transitoriedad y persistencia. Es así que la prueba electrónica tiende a ser más voluminosa, más difícil de destruir, fácilmente modificable, fácilmente duplicada, potencialmente más expresiva y fácilmente disponible.

En Argentina, la "Guía de obtención, preservación y tratamiento digital", elaborada por el Ministerio Público Fiscal de la República Argentina, considera a la evidencia digital "como el conjunto de datos e información, relevantes para una investigación, que se encuentra almacenada o es trasmitida por una computadora o dispositivo electrónico"[318].

5.4.1. Características de la Evidencia Digital

Estas características hacen que se haga más que nunca imprescindible contar con una adecuada cadena de custodia. Definida como aquel procedimiento, oportunamente documentado, que permite constatar la identidad, integridad y

[317] BIELLI, Gastón y ORDOÑEZ, Carlos, “La prueba electrónica: teoría y práctica”, 1a ed.- Ciudad Autónoma de Buenos Aires: La Ley, 2019.ISBN 978-987-03-3822-2

[318] MINISTERIO PÚBLICO FISCAL, Protocolos y Guías de Actuación, Disponible en url: https://www.mpf.gob.ar/ufeci/enlaces/protocolos-y-guias-de-actuacion/

autenticidad de los vestigios o indicios de un hecho relevante para el asunto, desde que son encontrados hasta que se aportan al proceso como pruebas[319].

Las características y diferencias más notables entre los elementos de prueba físicos y los datos informáticos, desarrolladas en el documento sobre tratamiento de la Evidencia Digital del Consejo de Europa[320] son:

- El dato informático no es visible para las personas sin conocimientos y formación técnica especial. De manera tal que requiere algún tipo de traducción tecnológica del formato digital para ser apreciada por los sentidos de los operadores del sistema penal o de cualquier persona. De esta manera, la información almacenada en los dispositivos informáticos no resulta de mucha utilidad para quienes no son especialistas debido a su carácter técnico y a la necesidad de conocimientos específicos para asegurar un tratamiento adecuado que evite alteraciones.
- El dato informático es muy frágil y volátil. En algunos casos, las pruebas electrónicas están almacenadas en dispositivos electrónicos en los que cualquier acción puede alterar su estado. El cambio en la memoria de los dispositivos puede ocurrir por alterar el estado original en el que se encontró un equipo (por ejemplo, apagarlo o encenderlo) lo que genera la necesidad de mecanismos especiales para asegurar la cadena de custodia de los datos.
- El contenido original puede ser alterado o destruido incluso mediante el uso habitual del dispositivo electrónico. El estado de la memoria de los dispositivos electrónicos cambia constantemente, ya sea por voluntad del usuario (“guardar documento”, “copiar archivo”) o bien automáticamente por el sistema operativo (“asignar espacio para programa”, “almacenamiento temporal de datos para intercambio entre dispositivos”).

[319] RAMÍREZ, E. Por qué es importante la cadena de custodia. 5 de julio de 2017. Recuperado de: https://idconline.mx/corporativo/2017/07/04/por-que-es-importante-la-cadena-de-custodia

[320] COUNCIL OF EUROPE; Guía de Prueba Electrónica..., elaborada por la Data Protection and Cybercrime Division del 7 Consejo de Europa, ob. cit, pág. 12 y ss; conclusiones de la International Telecommunication Union en Manual de Comprensión del Ciberdelito. Fenómenos, Dificultades y Respuestas Jurídicas, publicación de la versión en Español de Septiembre del año 2012

- Masividad de la información digital y dificultad para la búsqueda de la información pertinente para el objeto procesal. La capacidad creciente de almacenamiento de los dispositivos y el bajo costo económico que significa está generando un número cada vez mayor de documentos digitales. Sin perjuicio de las herramientas informáticas que permiten automatizar los procesos de búsqueda, la identificación de la evidencia digital pertinente en un dispositivo o sistema informático que puede transportar millones de documentos constituye un desafío logístico para los investigadores y un desafío para las garantías individuales por la posibilidad de encuentros causales (o no tan casuales) de información indiscriminada muchas veces alejada del objeto de prueba que habilitó una medida.
- La evidencia digital puede copiarse sin límites, en realidad, si la operación se efectúa correctamente y con los instrumentos necesarios no se trata propiamente de copias sino de una clonación ya que los nuevos resultados mantendrían todas las características del original. El contenido electrónico puede copiarse infinitas veces y ser exactamente igual al contenido original. Este atributo único permite realizar múltiples copias exactas al contenido original para ser distribuidas y analizadas por diversos especialistas al mismo tiempo (por ejemplo, puede entregarse una copia bit a bit a la defensa para que realice su propia pericia). De esta manera una correcta obtención de la prueba digital permite que todas las medidas sean siempre actos de prueba reproducibles, en términos procesales[321] .

Existen innumerables trabajos que desarrollan con profundidad técnica el tema de la evidencia digital, por lo que consideramos apropiado evitar un análisis técnico exhaustivo que excede el alcance para esta tesis, a fin de evitar seguir introduciendo tópicos en una temática que ya es lo suficientemente compleja.

[321] SALT, Marcos G., Tesis Doctoral, p. 20

5.4.2. La necesidad de nuevas reglas

Si bien en este punto afirmar que la Evidencia Digital NO es igual a la Evidencia Física parece ser de sentido lógico, la realidad es que (al menos en gran parte de los países incluídos en el estudio, sobre todo en Argentina) aún existe un importante esfuerzo en seguir aplicando un paradigma probatorio diseñado y pensado para el mundo físico, al mundo de la evidencia digital.

Ya en el año 2005, el profesor Orin S. Kerr, afirmaba a través de una investigación[322] que muestra cómo las normas de procedimiento penal existentes (al momento de su análisis por supuesto) están mal equipadas para regular la recopilación de pruebas digitales. En ese momento (año 2005) este reconocido autor predecía que las reglas de procedimiento penal iban a evolucionar (creándose nuevas) para regular las investigaciones de evidencia digital y ofrece ideas preliminares sobre cómo deberían ser esas reglas y qué instituciones deberían generarlas. Sostuvo con mucho acierto que las pruebas digitales tendrían como consecuencia la generación de nuevas normas de procedimiento penal porque los delitos informáticos presentan nuevos hechos que exigieron nuevas normativas de fondo.

Coincidimos plenamente en el razonamiento que así como el derecho procesal penal ha evolucionado para regular los mecanismos comunes a la investigación de delitos físicos, generando muchas medidas de investigación tendientes a la obtención de dicha evidencia, así también debería ocurrir lo mismo con respecto al ámbito digital.

En lo que insistimos, es en pensar que la integración de evidencia digital en el proceso penal plantea un desafío jurídico significativo en cuanto a la posible adaptación de los métodos de prueba tradicionales.

Desde nuestra óptica, la dificultad en la investigación del cibercrimen impulsa la necesidad de desarrollar nuevos medios de prueba (en el sentido de pensar fuera de la caja para poder probar los hechos), pero sobre todo, apuntar hacia la

[322] KERR, Orin S., Digital Evidence and the New Criminal Procedure. 105 Columbia Law Review 279 (2005), Disponible en SSRN: https://ssrn.com/abstract=594101

necesidad de contar con nuevas medidas de investigación que me permitan acceder a dichos datos.

Así, y como veremos en el próximo capítulo con más detalle, se comienza a hablar sobre el acceso transfronterizo de datos, accesos remotos, agente encubierto informático, el uso de software malicioso por parte del Estado, entre otras medidas.

A modo de corolario, está claro que en ese sinuoso camino de la regulación de medidas de investigación cada vez más invasivas, es que existen grandes posibilidades de afectación de garantías constitucionales, en especial, del derecho a la intimidad, por lo que se hace indispensable partir de un adecuado análisis y distinción entre lo que son medios probatorios, de las medidas de injerencia o coerción.

5.5. Medidas de injerencia (o coerción) y medios de prueba

Es importante para el objeto de la presente tesis que el lector pueda distinguir la diferencia entre medios de prueba con medidas de injerencia (o de coerción) a través de las cuales se puede incorporar elementos de prueba.

Un problema son los medios de prueba donde según como hemos visto anteriormente en este capítulo, en principio, rige la libertad probatoria. Otro problema a tener en cuenta es el sistema o modelo de valoración probatoria, distinguiendo si es tasada, sobre la sana crítica, o se apoya en libres convicciones.

Los sistemas procesales penales en Argentina, casi en su mayoría, proponen un sistema abierto en cuestiones probatorias. A modo de ejemplo, el Código Procesal de la Ciudad Autónoma de Buenos Aires en su Artículo 112 reza: "*Los hechos y las circunstancias de interés para la solución correcta del caso podrán acreditarse por cualquier medio de prueba que no resulte contrario a los principios contemplados en este Código*". A su vez, el Artículo 192 del Código Procesal Penal Cordobés (CPPC) establece que "*Todos los hechos y circunstancias relacionados*

con el objeto del proceso pueden ser acreditados por cualquier medio de prueba, salvo las excepciones previstas por las leyes" y el Artículo 193 del CPP de la Nación "*La instrucción tendrá por objeto: 1°) Comprobar si existe un hecho delictuoso mediante las diligencias conducentes al descubrimiento de la verdad*", entre otros.

En la práctica, excepto en algunas provincias que ya veremos en el próximo capítulo, Argentina ha tomado el camino de suplir la falta de regulación en el ámbito del derecho procesal penal en relación a la evidencia digital a través de la aplicación -a nuestro criterio abusiva- del principio de libertad probatoria.

Como hemos repasado en el punto 5.3.4, este principio se remonta a épocas pasadas en las que se buscaba superar el sistema de prueba tasada y, por ese motivo, se procuraba poder acceder a la verdad a través de cualquier medio que no vulnerara principios y garantías constitucionales. Entendemos que su aplicación, al menos en Argentina, se ha tornado abusiva toda vez que se ha malinterpretado (o forzado su interpretación para hacer decir a este principio algo que no dice) esta posibilidad legal de utilizar cualquier elemento como material probatorio, con la posibilidad de solicitar (y autorizar judicialmente) medidas de investigación (o sea, de injerencia) tendientes a conseguir ese material probatorio.

En este sentido, Gustavo Bruzzone[323], afirma que en relación a los medios de prueba, el sistema argentino sostiene un abierto: *numerus apertus*. Apoyado en el inciso 1º del art. 193 del Código Procesal Penal de la Nación, donde se afirma que se tendrán que utilizar todas "las diligencias conducentes al descubrimiento de la verdad". No obstante su postura de apertura, señala la existencia de una importante serie de limitaciones a esta apertura, distinguiendo lo que serían limitaciones concretamente establecidas por el legislador, de aquellas que surgen de principios generales. Entre aquellas limitaciones definidas especialmente por el código, menciona a modo de ejemplo a la prohibición de declaraciones entre parientes, regulada en el art. 242 del CPP de la Nación Argentina. Asimismo, con la prohibición de obtención de una confección a través de promesas o coacciones de algún tipo, regulada en el art. 296 CPP.

[323] BRUZZONE, Gustavo; "La nulla coactio sine lege como pauta de trabajo en materia de medidas de coerción en el proceso penal"; Estudios sobre Justicia Penal, Homenaje al Profesor Julio B. Maier, 2005.

Sin embargo, afirma el profesor Bruzzone que "*Siempre que la medida probatoria ponga en crisis derechos y garantías de manera directa nos encontraremos, en realidad, frente a una medida de coerción o de injerencia y, como tal, no es posible utilizarlos sin limitaciones".* Es decir, si bien existe una apertura en materia probatoria, no ocurre lo mismo con las medidas de coerción o de injerencia de las que puede derivar (o no) la incorporación de elementos probatorios.

En este sentido, el autor establece una importante diferencia entre medidas de coerción que suponen la incorporación de pruebas (por ejemplo un registro remoto), de aquellas que sólo tienden a la obtención de los fines del proceso y que, sólo en forma mediata, responden a una finalidad probatoria.

Ejemplo de esta segunda, donde se cumple este doble objetivo, podría mencionarse la medida del encarcelamiento preventivo, donde por un lado se justifica para neutralizar los peligros procesales (fuga y entorpecimiento de la investigación) y por otro, continuar con el intento de la averiguación de la verdad.

Volviendo a la diferencia planteada anteriormente, los medios probatorios en general no tienen ese grado de afectación de derechos y garantías, en tanto no lo afecten de manera directa en un derecho o en una garantía. Un ejemplo de estas, sería la incorporación de pruebas a través de una pericia informática realizada sobre un sistema informático que permite acreditar un acceso ilegítimo a un sistema o dato restringido.

En cambio, las medidas de coerción o de injerencia, suponen una afectación directa en contra de una garantía o derecho de la persona investigada. En este punto, el Dr. Bruzzone recuerda que así como el Derecho Penal sólo debe ser utilizado como *última ratio* para la resolución de conflictos sociales, también las medidas de coerción deben ser el último recurso y no la regla a seguir en lo que hace al proceso penal.

5.5.1. El origen del principio de Nulla coactio sine lege

El reconocido jurista español, Santiago Mir Puig desarrolla en una de sus obras[324] que los límites derivados del Estado de Derecho son consecuencia de lo que se conoce como "principio de legalidad". El principio de legalidad se expresa, en su aspecto formal, con el aforismo *"nullum crimen, nulla poena sine lege"*, procedente pese a su formulación latina, de *FEUERBACH* quien vino a reflejar y precisar una de las conquistas centrales de la Revolución Francesa (art. 8 de la Declaración de Derechos del Hombre de 26 de agosto de 1789 y de la Constitución de 3 de septiembre de 1791).

En su sentido actual, sostiene Mir Puig que el principio de legalidad se derivó en un principio de la teoría ilustrada del contrato social y presupone una organización política basada en la división de poderes, en la que la ley fuese competencia exclusiva de los representantes del pueblo. El ciudadano sólo admite el paso del estado de naturaleza al estado civil en virtud de un pacto -contrato social- en el que asegura su participación y control de la vida política de la comunidad. Tal participación tiene lugar por medio del Poder Legislativo, que representa -al menos teóricamente- al pueblo. Sólo de él puede emanar la ley, que constituye, pues, la expresión de la voluntad popular. Exigir que las penas se hallen previstas por la ley persigue, como se ve, que cuenten con el consenso de los ciudadanos, únicos legitimados para establecer las privaciones de derechos fundamentales que implican.

El principio de legalidad no es sólo, entonces, una exigencia de seguridad jurídica que permita sólo la posibilidad de conocimiento previo de los delitos y las penas, sino además la garantía de que el ciudadano no podrá verse sometido por parte del Estado ni de los jueces a penas que no admita el pueblo.

El principio nullum crimen, nulla poena sine lege, así entendido, pasó a inspirar las legislaciones en todas partes del mundo[325]. Las constituciones y códigos penales

[324] MIR PUIG, Santiago; "Introducción a las bases del derecho penal: Concepto y Método", Editorial BdF, 2003
[325] JIMÉNEZ DE ASÚA; "Tratado de Derecho Penal",Editorial Losada; ps. 388 y siguientes

españoles -desde el de 1822- siguieron este camino, y desde 1848 el principio de legalidad se formula de modo básicamente coincidente con la actual regulación.

Gustavo Bruzzone afirma[326] entonces que del principio constitucional de *nullum crimen, nulla poena sine lege,* se deriva el principio objeto de nuestro interés para el presente trabajo: el principio de la *nulla coactio sine lege*, traducido como la necesidad de constatación acerca de si la medida de coerción o de injerencia que se pretende aplicar, efectivamente se encuentra prevista en la ley procesal, y en su caso con qué alcance o para qué supuestos.

Es decir, que si tomamos una medida de coerción que ya sea que tenga efecto directamente probatorio o asegurativo del proceso, y dicha medida no se encuentra expresamente prevista, o bien lo está, pero no para esa clase de casos, entonces estamos violando el mandato del art. 18 de la Constitución Nacional (caso de Argentina[327]), toda vez que de dicha garantía constitucional y jurisdiccional se deriva el principio de *nullum crimen, nulla poena sine lege*, y de este último, el principio de *nulla coactio sine lege*.

A continuación, realizaremos un breve análisis de este importante principio.

5.5.2. Primer nivel de análisis: existencia y alcance de la medida

En un primer nivel de análisis, el autor plantea una revisión acerca de si dicha medida está prevista en el código procesal aplicable, y en el caso que la medida se encuentre regulada, nos invita a analizar y determinar si su aplicación es posible en todos los casos o por el contrario, se encuentra limitada para determinados casos (por ejemplo, para algunos tipos de delitos).

---

[326] BRUZZONE, Gustavo; "La nulla coactio sine lege como pauta de trabajo en materia de medidas de coerción en el proceso penal"; Estudios sobre Justicia Penal, Homenaje al Profesor Julio B. Maier, 2005.

[327] Constitución Nacional de Argentina, Artículo 18; "Ningún habitante de la Nación puede ser penado sin juicio previo fundado en ley anterior al hecho del proceso, ni juzgado por comisiones especiales, o sacado de los jueces designados por la ley antes del hecho de la causa."

En su trabajo el autor plantea el ejemplo de autorizar como medida de investigación (en Argentina), la disposición de un agente encubierto a una organización criminal dedicada a la violación de mujeres por motivos raciales. Bruzzone plantea con claridad que no se podría disponer de tal medida, toda vez que si bien está regulada, sólo está prevista por decisión del legislador nacional, para investigar determinados delitos (relacionadas a narcotráfico, terrorismo, etc.). Entonces como la medida de investigación del agente encubierto no está prevista para investigar el delito del ejemplo, considera inaplicable dicha medida y por lo tanto, su aplicación implicaría una afectación del principio objeto de análisis.

Otro ejemplo, esta vez más relacionado con el ámbito de la delincuencia informática y además, para plantear un caso más complejo, sería un caso donde la medida de investigación se encuentra efectivamente regulada en el Código Procesal Penal, pero no para los casos donde se están utilizando, como podría ser el caso de la medida de requisa.

Es decir, si bien existe como medida procesal, la misma no establece (por ejemplo en el Código Procesal Penal de la Provincia de Santa Fe) que pueda aplicarse a los datos informáticos, algo que actualmente puede observarse en una gran cantidad de órdenes de allanamientos, que incluyen la requisa de datos. Sin embargo, si el mismo caso es analizado bajo la luz de la aplicación del Código Procesal Penal Federal, dicha medida (o una parecida) si ha sido prevista por el legislador, a través del art. 151[328] que autoriza a la incautación de datos.

5.5.3. Segundo nivel de análisis: competencia objetiva

Habiendo superado el primer nivel, será preciso avanzar a un segundo nivel de análisis, donde Bruzzone invita a determinar si dicha medida de coerción o injerencia, efectivamente fue dictada por el órgano competente.

[328] Código Procesal Penal Federal; Art. 151: "El juez podrá ordenar a requerimiento de parte y por auto fundado, el registro de un sistema informático o de una parte de éste, o de un medio de almacenamiento de datos informáticos o electrónicos, con el objeto de secuestrar los componentes del sistema, obtener copia o preservar datos o elementos de interés para la investigación, bajo las condiciones establecidas en el artículo 136"

En este punto trabaja como ejemplo la medida de la requisa personal, cuestionando a aquellos casos de guardias de seguridad privada, que sin perjuicio del origen que tengan (ex policías por ejemplo) o si en otros aspectos de sus vidas son funcionarios públicos, en tanto son personas particulares, no están autorizados a llevar adelante dicha medida.

En materia de delitos informáticos, podemos citar los casos donde en el marco del desarrollo de la investigación penal preparatoria, desde la fiscalía se solicita por vía de una medida informativa, que un ISP provea información relacionada a datos de abonado sobre una determinada dirección IP, algo que por ejemplo ha sido intensamente debatido en un caso de Ciudad Autónoma de Buenos Aires en el contexto de una investigación sobre grooming[329]. En dicho caso, que más adelante desarrollaremos por otros aspectos de interés que se desarrollan en el mismo, plantea un cuestionamiento desde la defensa penal, que consideraba que era necesaria autorización judicial para que la fiscalía que llevó adelante la investigación pueda oficiar y acceder (sin contar con autorización judicial) a datos de abonado (BSI) que fueron determinantes para la detención de la persona acusada.

5.5.4. Tercer nivel de análisis: competencia subjetiva

En un tercer nivel de análisis, Bruzzone aborda que además de verificar que la medida sea correcta desde un punto de vista objetivo (segundo nivel) también debe determinarse si el órgano subjetivamente se encontraba en condiciones de dictar dicha medida. Es decir, la medida tiene que estar adecuadamente "justificada" o si por el contrario, la diligencia es solicitada de forma arbitraria o discrecional, sin justificación alguna.

A modo de ejemplo, señala el caso de policías que podrían detener a una persona por averiguación de antecedentes, pero que, si esos antecedentes ya habían sido verificados o constatados, no existiría justificación alguna para continuar

[329] Fallo "Ministerio Público —Fiscalía de Cámara Norte de la CABA— s/ queja por recurso de inconstitucionalidad denegado en 'A, C s/ infr. art. 128.2, párr. 2°, CP'"

con dicha detención o incluso, volver a detenerlo dentro de las 24 hs de la detención anterior.

Para ello, considera que será la fundamentación de la decisión de la medida la clave para poder confirmar si la medida supera este tercer nivel de análisis, en relación al aspecto subjetivo de su dictado. Para poder llevar adelante estos "controles" sobre la adecuada fundamentación de las medidas, el autor considera que para cada caso debemos constatar que la medida sea necesaria, idónea y proporcional.

A modo de síntesis y en esta aproximación a una especie de teoría general de las medidas de coerción generada por el Dr. Gustavo Bruzzone, el mismo nos propone (entendiendo la importancia de la aplicación de estos controles en la praxis procesal) una especie de método que ayude a constatar, respecto de cada media, si su aplicación es o no es adecuada:

1. *Nulla coactio sine lege*: (no hay medida de coerción sin ley)
2. Competencia del órgano que dispone la medida (aspecto objetivo y subjetivo)
3. Necesidad de la medida
4. Idoneidad de la medida para el fin que se persigue
5. Proporcionalidad de la medida, teniendo en cuenta los intereses afectados.

Teniendo como base estos principios mencionados por el autor, a continuación procederemos a realizar un breve desarrollo sobre estos y otros principios establecidos en la normativa procesal penal al respecto de las medidas de investigación.

Coincidiendo con esta línea, hasta hace pocos años, previo a la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, España atravesó por el mismo contexto que se puede ver en gran parte de la realidad latinoamericana.

Es decir que, acuciados por la desidia legislativa, los tribunales españoles actuaron comprometiendo el principio de legalidad, desde el momento que aplicaron medidas de investigación tecnológica, como por ejemplo, el registro de dispositivos

de almacenamiento masivo de información, sin sujeción a una legalidad que, por otro lado, era inexistente a pesar de ser muy necesaria. Se daba así por bueno el acto de investigación sobre uno de estos dispositivos cuando se encontraban en una entrada y registro que sí estaba autorizada, pero que no los mencionaba como posibles hallazgos. Así, en la que se calificaba como "línea jurisprudencial muy discutible sostenían que la ocupación y análisis de equipos informáticos hallados en el curso de una entrada y registro domiciliario no exigía que el mandamiento judicial contemplara expresamente tal eventualidad"[330].

Además, ha de tenerse en cuenta que el principio de legalidad no se cumplirá por la mera existencia de una ley que permita el acto de investigación tecnológica, sino que es preciso que esa ley delimite con suficiente precisión en qué situaciones puede tener lugar ese acto y hasta dónde se pueden violentar los derechos afectados. De este modo se preservará la seguridad jurídica de los justiciables como eventuales destinatarios de la medida.

En este sentido Velasco Núñez, señala que "la medida tecnológica que el juez autorice debe estar prevista por una norma que la habilite, que ha de ser de calidad tal que, por un lado, permita a todo ciudadano saber antes de acordarla en qué circunstancia se puede restringir su derecho y, por otro, evitar situaciones de abuso o arbitrariedad en los agentes del Estado al hacerlo". Concluye este autor diciendo que "el juez no podrá autorizar el uso de una medida tecnológica de investigación que no esté prevista en la ley, ni en circunstancias que vayan más allá de lo pretendido y permitido por la norma"[331].

El Tribunal Europeo de Derechos Humanos[332], interpretando el art. 8 CEDH estima que la injerencia del Estado en la vida privada puede resultar justificada siempre que concurran tres requisitos:

- Que la finalidad sea legítima (legitimidad del fin).
- Que la injerencia esté prevista por la ley (legalidad).

[330] MARCHENA GÓMEZ, M. y GONZÁLEZ-CUELLAR SERRANO, N.: La reforma de la Ley de Enjuiciamiento Criminal en 2015, Madrid, 2015, p. 212.
[331] VELASCO, Núñez, E.: Delitos tecnológicos: definición, investigación y prueba en el proceso penal, Madrid, 2016, p. 68
[332] STEDH (Sección 4ª) 3 de abril de 2007, caso Copland contra Reino Unido. STEDH (Gran Sala) 4 de mayo de 2000, caso Rotaru contra Rumanía.

- Y, por último, que sea necesaria en una sociedad democrática para la consecución de ese fin (necesidad)[2].

Esta doctrina ha sido recogida y desarrollada por la jurisprudencia constitucional española STC 115/2013, de 9 de mayo[333]. Estos presupuestos resultan plenamente aplicables a la injerencia en el derecho a la intimidad por aquellas diligencias de investigación que afectan al mismo, como puede ser el registro de un sistema informático.

5.6. La afectación de derechos a través de medidas de investigación penal

De acuerdo al Dr. Federico Fumis, las nuevas tecnologías han representado un profundo cambio, en tanto posibilitaron la incorporación de nuevos métodos investigativos y medios probatorios al proceso y -al mismo tiempo- permitieron potenciar la capacidad de viejos métodos y medios que, apoyados en los avances técnicos, resultan cada vez más eficaces. Sin embargo, no podemos avanzar en el desarrollo del tema sin dejar sentado que estos nuevos medios tecnológicos -junto a sus ventajas y posibilidades de éxito-, traen aparejada la posibilidad cierta de lesionar derechos y garantías constitucionales con gran facilidad y de un modo prácticamente invisible.

Como afirma el Dr. Fumis, "El descubrimiento de la verdad en el proceso penal se encuentra sometido a importantes limitaciones, como por ejemplo la prohibición de utilizar formas de investigación y pruebas que resulten violatorias de garantías consagradas en normas constitucionales y legales"[334].

En aspecto de fondo visibiliza una tensión (tan histórica como el derecho mismo) entre la eficacia de la investigación y el avance sobre los derechos y

[333] STC 70/2001 de 3 de abril [FJ 10] y la STC 173/2011, de 7 de noviembre [FJ 2º] y la jurisprudencia allí citada.
[334] FUMIS, Federico, "La utilización de modernas tecnologías en la persecución penal: su utilidad en la búsqueda de mayores índices", publicado en REDI: Revista Electrónica de Derecho Informático. Número 44

garantías constitucionales de la persona que está siendo investigada. Tensión, que a nuestro criterio se encuentra profundamente agravada por las nuevas tecnologías, toda vez que a diferencia de las medidas de investigación penal tradicionales, las nuevas tecnologías permiten avanzar sobre una esfera íntima de la persona de una forma mucho más "transparente" y rápida, haciendo que esta falta de tangibilidad de las barreras que delimitan estos bienes jurídicos tutelados constitucionalmente, puedan superarse con extrema facilidad en cuestión de segundos y en muchos casos, sin dejar mayores rastros.

En consecuencia, cada vez es más cotidiano encontrar ejemplos casos medidas de investigación penal, que por no contar con los requisitos jurídicos mínimos necesarios, podrían tornarse procesalmente inaprovechables por no respetar adecuadamente los derechos y las garantías procesales de las personas afectadas.

En el catálogo de derechos y garantías que pueden ser afectados a través de las distintas medidas de investigación, analizaremos la situación constitucional en Argentina y España (a modo comparativo).

Entre estos países podemos encontrar distintos derechos, como el secreto de las comunicaciones, derecho a la intimidad, derecho a la protección de los datos personales e incluso, del flamante derecho a la protección del propio entorno virtual, del cuál nos ocuparemos en este capítulo.

5.6.1. Las salvaguardas en el Convenio de Budapest

En este camino recorrido, es de una gran importancia destacar que el instrumento más importante a nivel internacional en la materia, como lo es el Convenio de Cibercrimen de Budapest, posee dentro su Sección 2 dedicada al Derecho Procesal, lo que consideramos una regulación bastante saludable para la protección de los derechos y garantías, bajo la regulación en el "Título 1: Disposiciones Comunes".

Bajo este título, se regulan los artículos 14 y 15 del Convenio que vienen a introducir diferentes tipos de límites: alcance, condiciones y garantías, aspectos que a continuación observaremos con más detalle.

	Convenio de Cibercrimen de Budapest
Art. 14	**Ámbito de aplicación de las medidas de derecho procesal** 1. Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para instaurar los poderes y procedimientos previstos en la presente sección a los efectos de investigación o de procedimientos penales específicos. 2. Salvo disposición en contrario, prevista en el artículo 21, los Estados podrán aplicar los poderes y procedimientos mencionados en el párrafo 1: a. a las infracciones penales establecidas en los artículos 2 a 11 del presente Convenio; b. a cualquier otra infracción penal cometida a través de un sistema informático; y c. a la recogida de pruebas electrónicas de cualquier infracción penal. 3. a. Los Estados podrán reservarse el derecho de aplicar la medida mencionada en el artículo 20 a las infracciones especificadas en sus reservas, siempre que el número de dichas infracciones no supere el de aquellas a las que se aplica la medida mencionada en el artículo 21. Los Estados tratarán de limitar tal reserva de modo que se permita la aplicación lo más amplia posible de la medida mencionada en el artículo 20. b. Cuando un Estado, en razón de las restricciones impuestas por su legislación vigente en el momento de la adopción del presente Convenio, no esté en condiciones de aplicar las medidas descritas en los artículos 20 y 21 a las comunicaciones transmitidas en un sistema informático de un prestador de servicios que i. es utilizado en beneficio de un grupo de usuarios cerrado, y ii. no emplea las redes públicas de telecomunicación y no está conectado a otro sistema informático, público o privado, ese Estado podrá reservarse el derecho de no aplicar dichas medidas a tales comunicaciones. Los Estados tratarán de limitar tal reserva de modo que se permita la aplicación lo más amplia posible de las medidas mencionadas en los artículos 20 y 21.
Art. 15	**Condiciones y garantías.** 1. Los Estados velarán para que la instauración, puesta en funcionamiento y aplicación de los poderes y procedimientos previstos en la presente sección se

	sometan a las condiciones y garantías dispuestas en su derecho interno, que debe asegurar una protección adecuada de los derechos del hombre y de las libertades y, en particular, de los derechos derivados de las obligaciones que haya asumido en aplicación del Convenio para la protección de los derechos humanos y libertades fundamentales del Consejo de Europa (1950) y del Pacto internacional de derechos civiles y políticos de Naciones Unidas (1966) o de otros instrumentos internacionales relativos a los derechos del hombre, y que debe integrar el principio de proporcionalidad. 2. Cuando ello sea posible, en atención a la naturaleza del poder o del procedimiento de que se trate, dichas condiciones y garantías incluirán, entre otras, la supervisión judicial u otras formas de supervisión independiente, la motivación justificante de la aplicación, la limitación del ámbito de aplicación y la duración del poder o del procedimiento en cuestión. 3. Los Estados examinarán la repercusión de los poderes y procedimientos de esta Sección sobre los derechos, responsabilidades e intereses legítimos de terceros, como exigencia dimanante del interés público y, en particular, de una correcta administración de justicia.

A nuestro criterio, consideramos de importancia valorar la incorporación de este tipo de articulado toda vez que son útiles para por un lado, determinar en qué casos podría considerarse la aplicación de las medidas de investigación que a posteriori se enuncian, y por otro, que es lo que más nos interesa dado el objeto de la presente tesis doctoral, para considerar que toda implementación a nivel interno de estas medidas, los Estados deberían asegurar una protección adecuada de los derechos del hombre y de las libertades.

En esta línea, nos parece de interés dejar constancia que sobre el final del inc. 1 se enuncia la integración del principio de proporcionalidad, sobre el cuál ya hemos ahondado previamente. Si bien participamos de la idea que hubiese sido una excelente oportunidad para realizar un mayor desarrollo de dicho principio, al menos rescatamos su enunciación.

Por otro lado, celebramos el hecho de mencionarse que los Estados deberían, siempre que sea posible y en atención a la naturaleza de la medida que se trate, se deberán establecer estos 4 aspectos claves:

- La existencia de supervisión judicial o de organismo independiente

- La existencia de una justificación que motive la adopción de dicha medida de investigación
- La limitación del ámbito de aplicación
- La duración del poder o del procedimiento en cuestión.

Como cierre en el art. 15 se menciona la obligación de los Estados de estar atentos a las consecuencia que la aplicación de las medidas de investigaciones reguladas puedan tener sobre los derechos, responsabilidades e intereses legítimos de terceros.

Como elemento extra, si bien responde a la normativa de un país fuera del alcance del presente trabajo, nos parece interesante mencionar cómo en el Artículo 57 de la Ley No. 53-07 sobre Crímenes y Delitos de Alta Tecnología de República Dominicana, se ha llegado a regular la "Desnaturalización del Proceso Investigativo", considerando que todos los actos desnaturalización de la investigación por parte de las autoridades competentes será castigada con la destitución inmediata del cargo, prisión de seis meses a cinco años y multa de no menos de diez salarios mínimos. Dentro de los actos de desnaturalización, se considerarán, entre otros:

> a) El inicio o solicitud de medidas por cualquier otra razón que no sea la persecución real de uno de los crímenes o delitos establecidos por la presente ley;
>
> b) El tráfico y comercialización de los datos obtenidos durante la investigación;
>
> c) La divulgación de datos personales y comerciales del procesado distintos a la naturaleza de la investigación, así como el tráfico o comercialización de los mismos.

Nos pareció de interés, considerar como más allá de la regulación de los principios de actuación, algunos países han optado por ir más allá y considerar como un delito penal, la utilización de dichas medidas de investigación fuera de las finalidades previstas, es decir, desnaturalizadas de su esencia.

5.6.2. Derecho a la privacidad e intimidad

El continuo desarrollo de las tecnologías de la información y las comunicaciones, constantemente nos obligan a repensar los alcance de un derecho tan histórico como el de la intimidad personal.

La posibilidad de tener tanta información personal en dispositivos como el celular o computadora, implican que su acceso coercitivo por parte del Estado en búsqueda de evidencia digital, implica un nivel de afectación más gravoso que por ejemplo, hubiese existido al acceder al contenido de una correspondencia epistolar (garantía expresamente reservada en la Constitución Nacional Argentina).

Siguiendo al maestro Marcos Salt, se trata de "un ámbito de intimidad personal construido y derivado de la particular vinculación entre las personas y los sistemas informáticos con los que se relacionan. De la mano de los avances tecnológicos y del mayor acceso por parte de la población a las herramientas informáticas y de telecomunicaciones se torna más evidente un vínculo diferente a lo conocido hasta ahora entre el hombre y las herramientas tecnológicas con las que interactúa"[335].

El texto constitucional de Argentina de 1853 prevé las garantías de privacidad e intimidad en dos artículos separados (CN, arts. 18 y 19). En nuestra doctrina constitucional, Carlos Nino[336] ha expuesto con claridad la diferencia entre los que denomina bienes de la privacidad e intimidad regulados de manera diferente en el texto constitucional: "*…privacidad entendida no como equivalente a intimidad sino en lo que se refiere a las acciones voluntarias de los individuos que no afecten a terceros…*". Con ello se refiere Nino a acciones privadas no en el sentido de que no deben ser accesibles al conocimiento público sino de que deben mantenerse incólumes de la injerencia estatal salvo que afecte a terceros. Resume la privacidad como la libertad de realizar cualquier acción que no cause daños a los demás, La intimidad, en cambio se refiere a una esfera de la persona que está exenta del conocimiento generalizado por parte de los demás.

[335] SALT, Marcos; Tesis Doctoral; pág. 106
[336] NINO, Carlos; Fundamentos de Derecho constitucional, pág. 304

En la misma línea podemos citar al Dr. Gustavo Garibaldi, quien afirma que denominará "*privacidad al derecho irrestricto de realizar, en todo tiempo y lugar, acciones que el Estado no puede prohibir porque carecen de aptitud para provocar daño a terceros. A su vez me referiré a la intimidad, como la esfera de la personalidad que cada uno puede mantener fuera del conocimiento generalizado*",

Sin perjuicio de ello, no se trataría de una superposición de normas constitucionales, sino que, por el contrario, se complementan. En lo que se refiere a la intimidad de comunicaciones el art. 19 de la CN protege de manera general las comunicaciones privadas que no afecten a terceros, protección absoluta que no admite límites. El maestro Julio Maier, afirmaba el carácter meramente académico de la discusión, pero que no incide en la presencia de la garantía independientemente del artículo constitucional en el que encuentre andamiaje ya sea como derivación del art. 19 o como aplicación extensiva del artículo 18[337].

El hecho de que no afecten a terceros las hace inviolables de forma absoluta y en el caso de que fueran conocidas por el Estado tornaría obligatorio devolverlas al estado anterior de intimidad, por ejemplo, destruyendo los registros. En el caso de que exista una afectación a terceros pierden la inmunidad total frente a injerencias del Estado pero no su carácter de íntimas, que las protege frente a ingresos arbitrarios del Estado o no respetuosos de las garantías impuestas[338].

El derecho a la privacidad en su acepción más amplia ha sido establecido en el artículo 19 de la CN de 1853 establece: "*Las acciones privadas de los hombres que de ningún modo ofendan al orden y a la moral pública, ni perjudiquen a un tercero, están sólo reservadas a Dios, y exentas de la autoridad de los magistrados. Ningún habitante de la Nación será obligado a hacer lo que no manda la ley, ni privado de lo que ella no prohíbe*".

Entendemos así que esta norma protege la privacidad en el sentido de mantener bajo protección un ámbito de protección del individuo que le permita realizar todas las acciones que no afecten a terceros, sea que ellas se realicen de

[337] Cf. MAIER, Julio, "DPPA", tomo III, especialmente nota 416.
[338] GARCÍA, Luis, La intervención de las comunicaciones telefónicas y otras telecomunicaciones en el Código Procesal Penal de la Nación: un cheque en blanco para espiar nuestra vida privada, publicado en "Cuadernos de Doctrina y Jurisprudencia Penal", nro. 6, 1997, editorial Ad Hoc, Buenos Aires, pág. 407 y ss.

manera privada o pública. Se trata de una inmunidad que protege a los ciudadanos de acciones del Estado que puedan intervenir o coartar la autonomía individual para cualquier idea pensamiento o actividad que no signifique una afectación a terceros (expresado en el texto del artículo constitucional como orden y moral pública).

Así, el artículo 19 de la CN refleja una idea más amplia que la de proteger el bien intimidad. Protege la privacidad como forma de plasmar los ideales de la concepción liberal en el plano de la autonomía personal garantizando todos aquellos bienes necesarios para asegurar la libre elección de un plan de vida sin interferencias estatales, salvo cuando afecte a terceros.

Asimismo, tal como ha sido rescatado por un sector de la doctrina, esta idea de privacidad permite también justificar la necesidad de garantizar la protección de la intimidad (en el sentido estricto de no conocimiento de terceros) de determinados datos o cuestiones cuando ellos puedan significar un menoscabo en la autonomía individual, cuestión que puede ser importante a los fines de esta investigación en la medida que resulta necesario analizar el resguardo de los ciudadanos frente a la intromisión del Estado en sus sistemas informáticos.

La protección de la intimidad está prevista en el art. 18 de la CN que reúne todas las garantías constitucionales frente al poder penal del Estado y que, en el párrafo pertinente, establece: "*…El domicilio es inviolable, como también la correspondencia epistolar y los papeles privados; y una ley determinará en qué casos y con qué justificativos podrá procederse a su allanamiento y ocupación*...". Así, el art. 18 garantiza la intimidad entendida como la posibilidad de excluir a terceros (incluido el Estado) del conocimiento de determinados hechos, circunstancias, comunicaciones o datos registrados en diferentes soportes. La norma se refiere de manera expresa a lo que sucede en un domicilio, lo que se registró en papeles privados o lo que se comunicó en una carta –correspondencia epistolar-, ello también es abarcado, por ejemplo, por el secreto bancario o fiscal y otros aspectos de la vida de un individuo, las comunicaciones telefónicas y otro tipo de comunicación mantenida por medios electrónicos como el correo electrónico o la

comunicación a través de voz ip[339]. Lo contrario implicaría dejar sin protección constitucional aspectos trascendentales para la intimidad de los ciudadanos como pueden ser sus conversaciones telefónicas y, más modernamente, las comunicaciones electrónicas y los documentos contenidos en soportes digitales.

Correctamente, en la interpretación dinámica de la CN, Alejandro Carrió sostiene una tesis amplia que parece adecuarse más a una interpretación teleológica del texto constitucional que tiene en cuenta no sólo la letra de la norma sino sus antecedentes y la ideología liberal que lo inspira y que tiene como fundamento la idea de que, aun con matices, los ámbitos de privacidad e intimidad de las personas deben ser protegidos para garantizar el libre desarrollo de la personalidad.

Julio Maier destaca el carácter no absoluto de la protección comparándolo con lo previsto en relación a la incoercibilidad del imputado como medio de prueba y la supresión de tormentos. Destaca que aun cuando los derechos y garantías no son absolutos (Artículo 28 de la CN Argentina), en el caso de la intimidad se trata de una de las garantías respecto de la cual el mismo texto constitucional concibe con limitaciones: "*…Al menos como principio no se concibe que lícitamente una persona sea torturada o sea coaccionada para que declare contra ella misma, pero está permitido entrometerse en la vida privada de una persona, allanando su domicilio, secuestrando su correspondencia epistolar o sus papeles privados, o interceptando sus comunicaciones, siempre que se respete las condiciones y exigencias que para ello prevé la ley común…*"[340].

La misma norma constitucional prevé supuestos admitidos de injerencia estatal y delega la regulación de los casos y las condiciones en que estas injerencias se pueden producir a la legislación. Esta materia es propia del desarrollo de las garantías 122 constitucionales en los códigos procesales penales. Las normas constitucionales referidas a la privacidad e intimidad, se han visto reforzadas en el bloque de constitucionalidad con la incorporación de los Pactos internacionales de Derechos Humanos. En ellos, la diferenciación entre privacidad e intimidad no

[339] CARRIÓ; Alejandro; "Garantías constitucionales en el Proceso Penal", 5 edición actualizada y 119 ampliada, Editorial Hammurabi, Buenos Aires, 2008, pág. 353 y ss.
[340] MAIER, Julio; Derecho Procesal Penal. Tomo I, pág. 681

aparece tan clara como en nuestro texto constitucional. Así la Convención Americana sobre Derechos Humanos lo prevé como una derivación de la protección a la honra y la dignidad humana en el artículo 11[341].

Es claro que la relación de las personas con los sistemas informáticos ha generado situaciones fácticas de potencial afectación a la intimidad antes impensada. Como explicamos anteriormente, actualmente se hace cotidiano el ingreso (con fines de registro y secuestro de datos) por parte del Estado al conocimiento de todo lo contenido en una computadora personal o en un teléfono inteligente de una persona sospechada de haber cometido un delito, podría llegar a exceder las posibilidades de injerencia en la intimidad que ese mismo acceso significa en un domicilio personal o la apertura de un maletín a los fines de su requisa y posterior secuestro de "papeles privados" útiles para la investigación.

Por este motivo, pudiera parecer en algunos casos errado que la analogía entre ambas situaciones fácticas (registro en un domicilio/registro en una computadora) sea una vía que permita proteger adecuadamente la garantía constitucional. El acceso al contenido de una computadora por parte del Estado permite un conocimiento de ámbitos de intimidad de las personas protegidos constitucionalmente mucho más comprensivo y profundo que el que permite el acceso y registro a un domicilio.

Debemos tener en consideración que el registro de una computadora o la memoria de un dispositivo celular podría permitir el conocimiento no solamente de los documentos existentes al momento en que se realiza la medida, sino que con un no muy complejo procedimiento técnico, sería posible también acceder a una serie de datos existentes en el pasado, que el propietario de dicho equipo eliminó por algún motivo, o incluso, datos de terceras personas que hubieran tenido contacto con el dispositivo en el pasado, como sucedió en el caso práctico del allanamiento a una empresa que comentaremos un poco más adelante (sección 5.7.5).

[341] *1. Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad. 2. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación*

Haciendo una pequeña digresión del tema, pero con mucha relación, Dicha posibilidad, debemos combinarla con una cotidiana (mala) práctica que se observa en la mayoría de las investigaciones penales, donde al momento de solicitar la extracción, los pedidos son tan amplios y difusos, que culminan en la realización de una extracción forense (física o lógica) de la totalidad de los datos del teléfono móvil, enviando la totalidad de dichos datos a la fiscalía para su revisión (evitando así la realización de los dictámenes forenses que deberían realizarse desde el laboratorio forense).

Es decir, que parte de los problemas de recursos (falta de personal capacitado, falta de capacidad operativa en los laboratorios forenses, etc.) terminan también repercutiendo en que la practicidad forense, termina con una afectación aún más amplia que la propia pretendida por el estado (toda vez que realizar una extracción completa, es un procedimiento más rápido que realizar una pericia forense más precisa de forma artesanal).

Volviendo al análisis jurídico que veníamos desarrollando, el acceso a los datos existente en un dispositivo personal permite acceder a elementos que posibilitan trazar perfiles personales y conocer gustos tendencias etc. (acceso a documentos electrónicos existentes e, incluso los borrados por el usuario aunque hubiera transcurrido un tiempo considerable; correos electrónicos, incluso aquellos que la persona hubiera decidido eliminar; tendencias y gustos personales y datos sensibles como tendencias religiosas, políticas, orientación sexual; páginas web visitadas; fotos y videos; manejo de cuentas bancarias; personas con las que se comunicó; películas vistas; interacción con otras personas en redes sociales, viajes realizados y planeados, etc.).

Fijando postura en este sentido, entendemos que no es que nos encontramos ante un “nuevo derecho” que necesita especial protección, sino que el bien jurídico afectado es siempre el mismo, con la diferencia que las tecnologías de la información actuales implican una manera nueva y mucho más potente de afectar el mismo derecho. En su caso, lo que entendemos debemos modificar, es un nivel de protección más adecuado para evitar la afectación más gravosa del mismo derecho.

El art. 8.1 del CEDH reconoce el derecho al respeto de la vida privada y familiar. En la Constitución Española, el derecho a la intimidad personal y familiar se regula en el artículo 18.1 junto al derecho al honor y a la propia imagen. Son tres derechos autónomos y sustantivos, aunque estrechamente vinculados entre sí, en tanto que derechos de la personalidad, derivados de la dignidad humana y dirigidos a la protección del patrimonio moral de las personas, por lo que estos tres derechos podrán verse afectados, de manera independiente, pero también, con frecuencia, de forma conjunta, dada su evidente proximidad.

La intimidad, también es un bien jurídico que la Constitución Española ha elevado a la categoría de derecho fundamental, vinculado con el libre desenvolvimiento de la personalidad y presupuesto del ejercicio potencial y pleno de otros derechos y libertades constitucionales[342].

El art. 18 CE acoge un contenido amplio de la intimidad personal y familiar que varía en función de las ideas y convicciones más generalizadas en la sociedad en cada momento histórico. La STC 115/2000, de 5 de mayo afirma que "el derecho fundamental a la intimidad reconocido por el art. 18.1 CE tiene por objeto garantizar al individuo un ámbito reservado de su vida, vinculado con el respeto a su dignidad como persona (art. 10.1 CE), frente a la acción y el conocimiento de los demás, sean éstos poderes públicos o simples particulares". De esta manera, la protección de ese ámbito reservado confiere a la persona el poder jurídico de imponer a terceros el deber de abstenerse de toda intromisión en la esfera íntima y la prohibición de hacer uso de lo así conocido.

Como ya hemos adelantado, considerando el nuevo universo de afectación de estos derechos, ha cobrado una gran importancia la necesidad de protección de la intimidad frente a los nuevos medios de investigación generados tras el desarrollo de las tecnologías, como aquellos que implican la utilización de la videovigilancia[343] o el

[342] MORALES PRATS, F. "Los delitos contra la intimidad en el Código Penal de 1995: reflexiones político-criminales", en Cuadernos de Derecho Judicial, volumen dedicado a "Estudios sobre el Código Penal de 1995 (parte especial)". Ed. CGPJ y la Escuela Judicial, Madrid, 1996, págs. 243 y ss.; y LÓPEZ ORTEGA, J. J. "La intimidad como bien jurídico protegido," en Cuadernos de Derecho Judicial, volumen dedicado a "Estudios sobre el Código Penal de 1995 (parte especial)" Ed. CGPJ y Escuela Judicial, Madrid, 1996, págs. 287 y ss.

[343] Desarrollada por la Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos.

uso de los dispositivos electrónico de captación y grabación de comunicaciones orales o de captación de la imagen, de seguimiento y de localización[344].

Resulta interesante destacar la Resolución N° 2013-2718, de fecha 15 de noviembre de 2013, del Tribunal De Apelación De Sentencia Penal Del Segundo Circuito Judicial De San José Costa Rica: "*Debe tenerse presente que vulnerar la intimidad de un sujeto, cuando mediante una orden de allanamiento ingresamos a su domicilio, es similar a ingresar a su información digitalizada, ya sea porque se secuestró un disco duro, una computadora o un teléfono celular. Acción que como tal se puede desplegar mediante acceso remoto. Pero sin importar la técnica utilizada, esa actuación debe revestirse con similares requisitos procesales y garantías que impidan injerencias arbitrarias en el ámbito de la intimidad. Igualmente, a cuando se accede a un domicilio mediante autorización y presencia judicial, a buscar rastros de la comisión de un hecho delictivo concreto, donde el titular de esos bienes figura como sospechoso*". En ese sentido, se ha pronunciado la jurisprudencia costarricense disponiendo que la orden de allanamiento de morada dictada por un juez penal no incluya la potestad de invadir distintos ámbitos de intimidad, como el contenido en documentos almacenados en medios electrónicos (llaves, maya, discos duros, teléfonos celulares, acceso a la nube, etc.). Mediante tal resolución, se aclaró a las partes que, durante la diligencia de registro, por parte del fiscal, se requiere la presencia del juez penal, para seleccionar así la información relevante según la investigación. En esa ocasión se estableció que el acceso a dichos dispositivos, "*… no es equiparable a la figura del registro que se prevé en la orden de allanamiento, pues el mismo alude al registro de la vivienda … y, en todo caso, si se aceptara que comprende el registro de los aparatos de cómputo o de almacenamiento de datos, con mayor razón debe practicarlo directa y personalmente el juez, aunque no lo haga en el mismo lugar y momento, sino en uno diferente, pues tal actuación no puede ser delegada, sino excepcionalísimamente (…), el espectro de protección de la intimidad para el domicilio es más reducido, en la actualidad, que ese otro, que puede tener importante cantidad de información (fotos, videos, conversaciones grabadas, etc.). La flexibilización de garantías, propia del Derecho Penal Moderno,*

[344] Regulado en el Título VIII del Libro II de la Ley de Enjuiciamiento Criminal "De las medidas de investigación limitativas de los derechos reconocidos en el artículo 18 de la Constitución", tras la modificación introducida por Ley Orgánica 13/2015, de 5 de octubre.

ha llevado a los operadores jurídicos a desconocer la literalidad de las normas, y el artículo 1 de la ley Nº 742530 es diáfano en cuanto establece la necesaria la presencia de juez. Hasta tanto no se reformule norma, la obligación existirá".[345]

Y agrega la resolución comentada .... "*Hoy es una realidad que mediante los dispositivos electrónicos se almacena la mayor parte de informaciones privadas y susceptibles de privacidad, por lo que la noción de documentos privados debe ensancharse. Así se lo ilustra el caso en mención: "En el presente asunto, no cabe duda de que las tarjetas SIM que se logran extraer de los celulares que se le decomisaron a los imputados constituyen una forma o medio de registrar información de carácter privado, pues por dicho medio –las tarjetas SIM– no solo existe la posibilidad de almacenar los datos relacionados con el servicio telefónico (datos del teléfono como lo sería el número), sino también otros datos o información de naturaleza privada que pertenece exclusivamente al usuario o dueño del teléfono". Es por ello que para su acceso y registro deben respetarse las normas procesales, so pena de que la información obtenida y las pericias que de ella deriven decanten en elementos probatorios inútiles para el proceso por violentar el derecho de la constitución y los derechos humanos."*[346]

5.6.3. Derecho al secreto de las comunicaciones

La protección del derecho al secreto de las comunicaciones tiene una entidad propia y diferenciada de su vinculación con el derecho a la intimidad, ya que las comunicaciones deberán resultar protegidas con independencia de su contenido.

En cuanto al alcance de lo que debe entenderse por "secreto de las comunicaciones", a través de una Sentencia[347] del Tribunal Constitucional, se ha reconocido que la misma "*garantiza a los interlocutores o comunicantes la confidencialidad de la comunicación telefónica que comprende el secreto de la*

[345] Op. Cit., Tribunal De Apelación De Sentencia Penal Del Segundo Circuito Judicial De San José Costa Rica. Resolución Nª 2013-2718, de 15 de noviembre de 2013.
[346] Tribunal De Apelación De Sentencia Penal Del Segundo Circuito Judicial De San José Costa Rica. Resolución Nª 2013-2718, de 15 de noviembre de 2013.
[347] Sentencia del Tribunal Constitucional 123/2002, de 20 de mayo

existencia de la comunicación misma y el contenido de lo comunicado, así como la confidencialidad de las circunstancias o datos externos de la conexión telefónica: su momento, duración y destino; y ello con independencia del carácter público o privado de la red de transmisión de la comunicación y del medio de transmisión –eléctrico, electromagnético u óptico, etc...– de la misma".

Bajo esta interpretación, coincidente con una importante Sentencia del año 1984[348] y la sentencia de otro reconocido fallo, como el Caso Malone[349], se sostuvo el criterio de interpretación amplia entendiendo que "*el concepto de secreto de la comunicación cubre no sólo el contenido de la comunicación, sino también la identidad subjetiva de los interlocutores*", y de esta forma el Tribunal otorgó el amparo al recurrente porque la entrega por la compañía telefónica a la Policía de los listados de llamadas del investigado no contaba con la preceptiva autorización judicial.

La jurisprudencia española establece[350] que el artículo 18.3 CE tiene un contenido puramente formal, que protege tanto de las intromisiones de los poderes públicos como de los particulares[351]. Siguiendo la jurisprudencia del Tribunal Constitucional, el 18.3 de la CE consagra la libertad de las comunicaciones y garantiza su secreto, sea cual fuere la forma de interceptación, mientras dure el proceso de comunicación, en el marco de comunicaciones indirectas, y frente a terceros ajenos a la comunicación. En este sentido, el secreto de la comunicación se vulnera no sólo con la interceptación de la misma, sino también con el simple conocimiento antijurídico de lo comunicado[352].

Aunque el artículo 18.3 CE menciona expresamente, las comunicaciones postales, telegráficas o telefónicas, dado el carácter abierto de su enunciado, se entienden comprendidas también otro tipo de comunicaciones como pueda ser el correo electrónico, chats o mensajería instantánea, u otros medios en los que se use

[348] STC 114/1984
[349] Sentencia del Tribunal Europeo de Derechos Humanos de 2 de agosto de 1984 (caso Malone)
[350] STC 114/1984, de 29 de noviembre; 281/2006, de 9 de octubre; SSTS 208/2006, de 20 de febrero y 309/2015, de 22 de mayo.
[351] STC 123/2002, de 20 de mayo "En una sociedad tecnológicamente avanzada como la actual, el secreto de las comunicaciones constituye no sólo garantía de libertad individual, sino instrumento de desarrollo cultural, científico y tecnológico colectivo".
[352] STC 114/1984, de 29 de noviembre; 49/1999, 5 de abril; 70/2002, 3 de abril; 184/2003, de 23 de octubre y 281/2006, de 9 de octubre

algún artificio instrumental o técnico[353] y la presencia de un elemento ajeno a aquéllos entre los que media el proceso de comunicación es indispensable para configurar el ilícito constitucional del precepto. En consecuencia, el levantamiento del secreto por uno de los intervinientes no se consideraría violación del artículo 18.3 CE, sino, en su caso, vulneración del derecho a la intimidad[268].

Además, el secreto cubre tanto el contenido de la comunicación como la identidad subjetiva de los interlocutores, por lo que a modo de ejemplo, queda afectado por este derecho tanto la entrega de los listados de llamadas telefónicas por las compañías telefónicas como también el acceso al registro de llamadas entrantes y salientes grabadas en un teléfono móvil. Asimismo, el acceso a determinados datos o aspectos externos de la comunicación que pueden encontrarse en el propio dispositivo electrónico (como ocurre con los registros almacenados en archivos temporales) también se encuentra amparado por el derecho fundamental al secreto de las comunicaciones.

Igualmente, en las comunicaciones a través de dispositivos electrónicos puede afirmarse que el derecho fundamental al secreto de las comunicaciones ampara también los datos que acompañan al proceso de comunicación; esto es, *cualesquiera datos informáticos relativos a una comunicación por medio de un sistema informático, generados por un sistema informático como elemento de la cadena de comunicación, que indiquen el origen, destino, ruta, hora, fecha, tamaño y duración de la comunicación o el tipo de servicio subyacente*[354].

La protección de este tipo de comunicaciones supone que no podrá interferirse o intervenirse la comunicación de cualquier persona salvo resolución judicial y con las garantías previstas. Al existir una reserva jurisdiccional, es siempre exigible la previa autorización judicial con los requisitos ya examinados.

---

[353] GONZÁLEZ PÉREZ, J. J. Utilización en el proceso penal de datos vinculados a las comunicaciones electrónicas recopilados sin indicios de comisión delictiva en "Protección de datos y proceso penal". Ed. La Ley, 2010, pág. 356 se refiere a las comunicaciones telemáticas como los servicios de comunicación que permite Internet, incluyendo el correo electrónico; la mensajería instantánea (servicio IRC, servicio ICQ, la voz sobre IP-VoIP, la videoconferencia y el envío de archivos en muchas ocasiones tipo P2P); los foros y blogs; y la navegación a través de internet.

[354] Definición de datos sobre el tráfico contenida en el art. 1 d) Convenio sobre Ciberdelincuencia de Budapest

Por el lado de Argentina, en el conocido Fallo Halabi[355], la Corte Suprema de Justicia de la Nación (CSJN) declaró la inconstitucionalidad de la Ley 25.873 y su decreto reglamentario, en el cuál se pretendía regular la retención de datos. En el fallo, y con relación a la interpretación sobre la protección constitucional de las comunicaciones, la CSJN expresó: "En relación con los aspectos reseñados resulta oportuno señalar que las comunicaciones a las que se refiere la ley 25.873 y todo lo que los individuos transmiten por las vías pertinentes integran la esfera de intimidad personal y se encuentran alcanzadas por las previsiones de los artículos 18 y 19 de la Constitución Nacional. El derecho a la intimidad y la garantía consecuente contra su lesión actúa contra toda "injerencia" o "intromisión" "arbitraria" o "abusiva" en la "vida privada" de los afectados (conf. art. 12 de la Declaración Universal de Derechos Humanos y art. 11, inc. 2°, de la Convención Americana sobre Derechos Humanos Tratados, ambos, con jerarquía constitucional en los términos del art. 75, inc. 22, de la Constitución Nacional y art. 1071 bis del Código Civil)."

En relación al caso concreto que se discutía en Halabi, también de interés para el marco de este trabajo en relación a la posibilidad de guarda de los datos de las comunicaciones, la Corte afirmó: "Es evidente que lo que las normas cuestionadas han establecido no es otra cosa que una restricción que afecta una de las facetas del ámbito de la autonomía individual que constituye el derecho a la intimidad, por cuanto sus previsiones no distinguen ni precisan de modo suficiente las oportunidades ni las situaciones en las que operarán las interceptaciones, toda vez que no especifican el tratamiento del tráfico de información de Internet en cuyo contexto es indiscutible que los datos de navegación anudan a los contenidos", reconociendo de esta forma una afectación al derecho de la intimidad sobre los usuarios.

Adicionalmente a este reconocimiento constitucional, existe un refuerzo sobre la protección sobre el secreto de las comunicaciones dentro de la Ley Nacional de Inteligencia de Argentina, Nº 25.520, donde reconoce la inviolabilidad de las comunicaciones:

[355] Sentencia CSJN: Halabi, Ernesto c/ P.E.N. - ley 25.873 - dto. 1563/04 s/ amparo ley 16.986

ARTICULO 5° — Las comunicaciones telefónicas, postales, de telégrafo o facsímil o cualquier otro sistema de envío de objetos o transmisión de imágenes, voces o paquetes de datos, así como cualquier tipo de información, archivos, registros y/o documentos privados o de entrada o lectura no autorizada o no accesible al público, son inviolables en todo el ámbito de la República Argentina, excepto cuando mediare orden o dispensa judicial en sentido contrario.

Similar regulación tiene la Ley Nacional de Telecomunicaciones Nº 19.728, en cuyos artículos 18 y 19 respectivamente afirma:

Art. 18. — La correspondencia de telecomunicaciones es inviolable. Su interceptación solo procederá a requerimiento de juez competente.

Art. 19. — La inviolabilidad de la correspondencia de telecomunicaciones importa la prohibición de abrir, sustraer, interceptar, interferir, cambiar su texto, desviar su curso, publicar, usar, tratar de conocer o facilitar que otra persona que no sea su destinatario conozca la existencia o el contenido de cualquier comunicación confiada a los prestadores del servicio y la de dar ocasión de cometer tales actos.

5.6.4. Derecho a la protección de datos personales

La protección de los datos personales a la cuál hace referencia el inciso 4 del art. 18 ya citado de la Constitución Española, posee un amplio desarrollo normativo y doctrinario, expandido aún más a través de la flamante normativa del Reglamento General de Protección de Datos[356], que entró en vigencia el 25 de Mayo de 2018, incorporando y profundizando aún más los derechos a la privacidad de los usuarios de servicios de comunicación.

Una primera interpretación llevó a considerar este derecho como una especificidad del derecho a la intimidad, aunque el Tribunal Constitucional ha considerado en la STC 254/1993, de 20 de julio y STC 290/2000, de 30 de noviembre que el derecho fundamental a la protección de datos personales (arts. 10 y 18.4 CE) es un derecho independiente, pero estrechamente relacionado con aquél;

[356] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (Texto pertinente a efectos del EEE)

es un derecho autónomo que faculta a la persona a controlar sus datos personales y la capacidad para disponer y decidir sobre los mismos.

La STC 94/1998, de 4 de mayo señaló que "*nos encontramos ante un derecho fundamental a la protección de datos por el que se garantiza a la persona el control sobre sus datos, cualesquiera datos personales, y sobre su uso y destino, para evitar el tráfico ilícito de los mismos o lesivo para la dignidad y los derechos de los afectados; de esta forma, el derecho a la protección de datos se configura como una facultad del ciudadano para oponerse a que determinados datos personales sean usados para fines distintos a aquél que justificó su obtención*".

Mediante la protección de este derecho se intenta lograr la adecuación y exactitud de las bases de datos y la cancelación cuando dejen de ser necesarios, así como el conocimiento y la posibilidad de acceso por parte de los afectados, con un especial deber de protección para los datos denominados sensibles, aquellos que afectan a la ideología, religión o creencias (art. 16.2 CE) y los relativos a la salud. Entendemos que derecho se halla estrechamente vinculado con la libertad ideológica, toda vez que evidentemente el almacenamiento y la utilización de datos informáticos puede suponer un riesgo para aquélla, no solamente por lo que se refiere a datos sensibles (entre los que se encuentran los de carácter ideológico o religioso), sino también por su posible utilización ajena a las finalidades para los que fueron recabados[357], o la inclusión de datos sin conocimiento del afectado[358], o el riesgo puede provenir por efectuarse accesos indebidos a ficheros ajenos[359].

En definitiva, la protección de datos no alude sólo a la reserva con la que se han de tratar ciertas informaciones, sino que viene fundamentalmente caracterizada por el reconocimiento a todos los ciudadanos de un poder de control sobre sus propios datos, en todo momento y dondequiera se encuentren. Ello permite hablar de un poder de control que desde el punto de vista activo tiene un carácter individualizado, pero también difuso, y desde el punto de vista pasivo va dirigido frente a todos aquellos sujetos que disponen de datos de carácter personal.

[357] SSTC 11/1998, de 13 de enero; 44 y 45/1999, de 22 de marzo, entre otras, en relación con la libertad sindical
[358] STC 202/1999, de 8 de noviembre
[359] STC 144/1999, de 22 de julio, en torno a una indebida utilización por parte de una Junta Electoral de Zona de datos incluidos en el Registro Central de Penados y Rebeldes

En la doctrina española, el autor Pérez Gil sostiene que la fase de investigación del proceso penal constituye una continuada intromisión en el ámbito de tutela que propicia toda la normativa de protección de datos personales, y critica que el acceso a datos personales por parte de la policía y su tratamiento, sea una actividad que integra hoy habitualmente sus funciones, pues constituye una forma de actuación completamente al margen de la actividad jurisdiccional (y ni siquiera de la del Ministerio Fiscal)[360].

Este autor defiende también que ni siquiera el Tribunal Supremo otorga la relevancia requerida a la materia que nos ocupa, tal y como acredita la copiosa jurisprudencia relativa a peticiones de registros y listados de llamadas, que aún admitiendo que no afectan al secreto de las comunicaciones, nadie tiene dudas que tales listados pueden contener datos de carácter personal.

En el 2004, el Alto Tribunal Español resolvió considerar bastante una providencia sin motivación alguna para acordar su solicitud, o no delimita con la suficiente nitidez conceptos esenciales de la normativa de protección de datos que sin embargo entiende de aplicación. Entre los argumentos, consideraron un dictamen de la Agencia de Protección de Datos fechado en 1999 vino a convalidar la idoneidad de las solicitudes de datos efectuadas por la Policía Judicial sin mandamiento judicial o requerimiento previo del Ministerio Fiscal, un fundamento al que todavía hoy se siguen aferrando los cuerpos policiales en sus requerimientos de aportación de datos. De todas maneras, el propio Pérez Gil reconoce que una cosa es que no nos hallemos en el ámbito del art. 18.3 CE, pero otra muy diferente es sostener que en absoluto estamos ante un derecho fundamental a fin de excluir del monopolio jurisdiccional la adopción y control de aquellas medidas que pudieran vulnerarlo o devaluarlo[361].

Otro interesante problema se refiere a si los datos obtenidos para investigar un hecho delictivo concreto podrían ser utilizados, sin previa autorización judicial, para la investigación de otras infracciones penales, o ser usados para la llamada búsqueda entrecruzada de rasgos distintivos (es decir, para comparar

[360] PÉREZ GIL, J. "Investigación penal y nuevas tecnologías (…) ob. cit. pág. 228.
[361] PÉREZ GIL, J. "Investigación penal y nuevas tecnologías (…) ob. cit. pág. 229.

automatizadamente los datos de personas que tienen determinadas características coincidentes con las del presunto autor del delito con la finalidad de centrar las pesquisas en determinados sujetos).

Tal cuestión ha quedado resuelta en la Ley de Enjuiciamiento Criminal toda vez que exige que se solicite del juez competente autorización para recabar la información que conste en los archivos automatizados de los prestadores de servicios, incluida la búsqueda entrecruzada o inteligente de datos, siempre que se precisen la naturaleza de los datos que hayan de ser conocidos y las razones que justifican la cesión.

Incluso, en la misma normativa, bajo el tratamiento del problema que suponía para el derecho a la protección de datos y para el derecho a la intimidad, el destino de todo el material electrónico usado en la investigación cuando ya no es imprescindible o es irrelevante para la investigación, ha dispuesto, una vez que se ponga término al procedimiento mediante resolución firme, el borrado y eliminación de los registros originales que puedan constar en los sistemas electrónicos e informáticos utilizados en la ejecución de la medida[362], conservándose una copia por el Letrado de la Administración de Justicia que será destruida a los cinco años desde que la pena se haya ejecutado o cuando el delito o la pena hayan prescrito o se haya decretado el sobreseimiento libre o haya recaído sentencia absolutoria firme respecto del investigado, dictando los Tribunales las órdenes oportunas a la Policía Judicial para que lleve a efecto la destrucción.

5.6.5. Derecho al entorno digital

En estos últimos años se viene afirmando por parte de algunos autores[363] la existencia de un nuevo derecho a “la identidad virtual”, nacido precisamente del uso de las nuevas tecnologías.

[362] Ley de Enjuiciamiento Criminal Española, artículo 588 bis k. Destrucción de registros.
[363] ZARAGOZA TEJADA, J. I., “La reforma operada por Ley 13/2015. El Agente Encubierto Informático”.ob. cit. pág 5. VALVERDE MEGÍAS, R., “Intervención de comunicaciones telemáticas y registro remoto”.ob.cit. pág. 26 CONDE-PUMPIDO TOURÓN, C. “La reforma procesal. Registro de sistemas informáticos, ampliación del registro a otros sistemas(…) ob. cit. pág. 5.

Este nuevo derecho, cuyo germen doctrinal puede encontrarse en la STC 173/2011, de 7 de noviembre, abarcaría una serie de elementos comunes del derecho a la intimidad, secreto de las comunicaciones y del derecho de protección de datos personales. Se fundamenta en la consideración de que los datos obtenidos de la interacción de una persona a través de las nuevas tecnologías, individualmente considerados o estudiados, no revelan ningún aspecto íntimo de la misma, pero si son estudiados en su conjunto, una vez analizados, pueden llegar a describir aspectos realmente relevantes de la personalidad de su titular[364].

No se puede tratar al ordenador y en general, a los dispositivos tecnológicos de almacenamiento de información, como si fueran una pieza de convicción más, pues en ellos coexisten datos técnicos y datos personales susceptibles de protección constitucional en el ámbito del derecho a la intimidad y la protección de datos (art. 18.1 y 4 de la CE). Pero su contenido también puede albergar información esencialmente ligada al derecho a la inviolabilidad de las comunicaciones (art. 18.3), como es el correo electrónico, que cuando es leído por su destinatario está amparado por el derecho a la intimidad. En este sentido, se afirma el "derecho al propio entorno virtual", integrado por todos esos datos que individualmente considerados, están protegidos por algunos de los derechos fundamentales convergentes antes indicados, pero que precisamente por su interrelación alrededor de un mismo titular de derechos y datos, precisan de un tratamiento unitario.

Este criterio ya puede apreciarse en la doctrina jurisprudencial de la Sala Segunda del Tribunal Supremo. Así, en la STS 342/2013, del 17 de abril, se habla expresamente ya del derecho al propio entorno virtual y se justifica en la misma una cita de cierta amplitud: "*El acceso de los poderes públicos al contenido del ordenador de un imputado, no queda legitimado a través de un acto unilateral de las*

[364] STC 173/2011, de 7 de noviembre.*"(…) Es evidente que cuando su titular navega por Internet, participa en foros de conversación o redes sociales, descarga archivos o documentos, realiza operaciones de comercio electrónico, forma parte de grupos de noticias, entre otras posibilidades, está revelando datos acerca de su personalidad, que pueden afectar al núcleo más profundo de su intimidad por referirse a ideologías, creencias religiosas, aficiones personales, información sobre la salud, orientaciones sexuales, etc. Quizás, estos datos que se reflejan en un ordenador personal puedan tacharse de irrelevantes o livianos si se consideran aisladamente, pero si se analizan en su conjunto, una vez convenientemente entremezclados, no cabe duda que configuran todos ellos un perfil altamente descriptivo de la personalidad de su titular, que es preciso proteger frente a la intromisión de terceros o de los poderes públicos, por cuanto atañen, en definitiva, a la misma peculiaridad o individualidad de la persona.*"

fuerzas y cuerpos de seguridad del Estado. El ordenador y, con carácter general, los dispositivos de almacenamiento masivo, son algo más que una pieza de convicción que, una vez aprehendida, queda expuesta en su integridad al control de los investigadores. El contenido de esta clase de dispositivos no puede degradarse a la simple condición de instrumento recipiendario de una serie de datos con mayor o menor relación con el derecho a la intimidad de su usuario. En el ordenador coexisten, es cierto, datos técnicos y datos personales susceptibles de protección constitucional en el ámbito del derecho a la intimidad y la protección de datos (art. 18.4 de la CE). Pero su contenido también puede albergar información esencialmente ligada al derecho a la inviolabilidad de las comunicaciones. El correo electrónico y los programas de gestión de mensajería instantánea no son sino instrumentos tecnológicos para hacer realidad, en formato telemático, el derecho a la libre comunicación entre dos o más personas. Es opinión generalizada que los mensajes de correo electrónico, una vez descargados desde el servidor, leídos por su destinatario y almacenados en alguna de las bandejas del programa de gestión, dejan de integrarse en el ámbito que sería propio de la inviolabilidad de las comunicaciones. La comunicación ha visto ya culminado su ciclo y la información contenida en el mensaje es, a partir de entonces, susceptible de protección por su relación con el ámbito reservado al derecho a la intimidad, cuya tutela constitucional es evidente, aunque de una intensidad distinta a la reservada para el derecho a la inviolabilidad de las comunicaciones. Por ello deviene necesario establecer una serie de garantías frente a los riesgos que existen para los derechos y libertades públicas, en particular la intimidad personal, a causa del uso indebido de la informática así como de las nuevas tecnologías de la información".

La ponderación judicial de las razones que justifican en el marco de una investigación penal el sacrificio de los derechos de los que es titular el usuario del ordenador, ha de hacerse sin perder de vista la multifuncionalidad de los datos que se almacenan en dicho dispositivo. Por lo que su tratamiento jurídico puede llegar a ser más adecuado si los mensajes, las imágenes, los documentos y, en general, todos los datos reveladores del perfil personal, reservado o íntimo de cualquier encausado, se contemplan de forma unitaria. Y es que, más allá del tratamiento constitucional fragmentado de todos y cada uno de los derechos que convergen en

el momento del sacrificio, existiría un auténtico derecho al propio entorno virtual. En él se integraría, sin perder su genuina sustantividad como manifestación de derechos constitucionales de nomen iuris propio toda "la información en formato electrónico que, a través del uso de las nuevas tecnologías, ya sea de forma consciente o inconsciente, con voluntariedad o sin ella, va generando el usuario, hasta el punto de dejar un rastro susceptible de seguimiento por los poderes públicos". Surge entonces la necesidad de dispensar una protección jurisdiccional frente a la necesidad del Estado de invadir ese entorno digital en el ámbito de la investigación de los ciberdelitos[365].

En la normativa española, el reconocimiento del "entorno virtual propio", incluso como derecho fundamental de nueva generación, queda plasmado en la STS 204/2016 de 10 de marzo, que al analizar el artículo 588 sexies b de la Ley de Enjuiciamiento Criminal (relativo al registro de dispositivos de almacenamiento masivo de información), dispone que "*el legislador otorga un tratamiento unitario a los datos contenidos en los ordenadores y teléfonos móviles, reveladores del perfil personal del investigado, configurando un derecho constitucional de nueva generación que es el derecho a la protección del propio entorno virtual*".

Sea como fuere, lo cierto es que tanto desde la perspectiva unitaria del derecho al entorno virtual propio, como de la perspectiva diversa de las garantías constitucionales exigidas para el sacrificio de los derechos a la inviolabilidad de las comunicaciones y a la intimidad, la intervención de un ordenador para acceder a su contenido exige un acto jurisdiccional habilitante. Y esa autorización no está incluida en la resolución judicial previa para acceder al domicilio en el que aquellos dispositivos se encuentran instalados. De ahí que, ya sea en la misma resolución, ya en otra formalmente diferenciada, el órgano jurisdiccional habrá de exteriorizar en su razonamiento que ha tomado en consideración la necesidad de sacrificar, además del domicilio como sede física en el que se ejerce el derecho a la intimidad personal, aquellos otros derechos que convergen en el momento de la utilización de las nuevas tecnologías.

[365] En el mismo sentido, ver Sentencia STS 985/2009, de 13 diciembre; 342/2013, de 17 de abril; 97/2015, de 24 de febrero.

En definitiva, toda investigación criminal (ya sea en el marco de un proceso penal ya iniciado o en el curso todavía de las diligencias policiales previas a la incoación del procedimiento) relacionada con las nuevas tecnologías, ha de desarrollarse con la máxima cautela y prudencia, y teniendo en cuenta siempre la importante incidencia que estas medidas de investigación puede tener en el contenido esencial de los derechos fundamentales reconocidos.

5.7. Principios aplicables a medidas de investigación

Siguiendo la línea del Artículo 588 bis a. de la Ley de Enjuiciamiento Criminal Española, se afirma que durante la instrucción de las causas se podrá acordar alguna de las medidas de investigación reguladas siempre que medie autorización judicial dictada con plena sujeción a los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad de la medida.

Es decir, encontramos en la normativa española, además de los tres principios mencionados previamente por el Dr. Bruzzone -principios de necesidad, idoneidad y proporcionalidad-, se requieren la existencia del principio de especialidad y excepcionalidad, dotando aún de mayor nivel de garantías a la aplicación de medidas de investigación.

5.7.1. Principio de especialidad

El art. 588 bis a núm. 2 LECrim establece que el principio de especialidad exige que una medida esté relacionada con la investigación de un delito concreto. Añadiendo a continuación, que no podrán autorizarse medidas de investigación tecnológica que tengan por objeto prevenir o descubrir delitos o despejar sospechas sin base objetiva.

De la dicción literal del precepto se desprenden dos rasgos configuradores del contenido del principio. El primero, desde un punto de vista positivo, se concreta en la exigencia de relación de la medida con la investigación de un delito determinado. El segundo, desde un punto de vista negativo, plantea tres posibles escenarios en los que la especialidad no se cumpliría: cuando la medida tenga por objeto prevenir delitos, cuando pretenda descubrirlos o cuando se dirija a despejar sospechas sin base objetiva. Y, efectivamente, en cualquiera de esos tres supuestos no existiría conexión alguna con un delito concreto.

Conviene detenernos en la afirmación positiva de la especialidad, es decir, en la relación de la medida de investigación con un delito concreto, porque cabe preguntarse hasta qué punto ha de estar identificado ese delito para que el principio de especialidad pueda estimarse cumplido.

La STC 26/2010, de 27 de abril[366], nos proporciona en su fundamento jurídico segundo una certera respuesta al describir cuál ha de ser la calidad de los indicios del delito que la sentencia comienza calificando como datos objetivos. Estos indicios, dice el Tribunal: "*(…) son algo más que simples sospechas, pero también algo menos que los indicios racionales que se exigen para el procesamiento, en este sentido, hemos reiterado que la relación entre la persona investigada y el delito se manifiesta en las sospechas que, como tiene declarado este Tribunal, no son tan sólo circunstancias meramente anímicas, sino que precisan para que puedan entenderse fundadas, hallarse apoyadas en datos objetivos que han de serlo en un doble sentido. En primer lugar, en el de ser accesibles a terceros sin lo que no serían susceptibles de control y, en segundo lugar, en el de que han de proporcionar una base real de la que pueda inferirse que se ha cometido o que se va a cometer el delito sin que puedan consistir en valoraciones acerca de la persona*".

Retomando la pregunta que nos hacíamos antes, habrá que contestar que el delito se considerará suficientemente identificado siempre que los indicios delictuales cumplan las dos condiciones que la sentencia exige: primero, accesibilidad y control por terceros y segundo, base real desconectada de valoraciones personales.

[366] STC 26/2010, de 27 de abril (RTC 2010, 26).

Concretado el primer rasgo definidor del contenido del principio, pasemos ahora a considerar una parte del segundo que se formula como una prohibición. El hecho de que art. 588 bis a núm. 2 LECrim no permita medidas de investigación tecnológica que tengan por objeto prevenir o descubrir delitos, no significa que estas actuaciones no pueda llevarlas a cabo la policía en cumplimiento legítimo de sus funciones siempre que no afecten a derechos fundamentales. La prohibición se ciñe al supuesto de las medidas de investigación tecnológica vulneradoras de tales derechos y a ese ámbito debe restringirse. La posible duda quedó claramente despejada por la SAN 20/2016, 18 de julio[367]. En ella, el Alto Tribunal refirió que la defensa, en el caso de autos, cuestionó la investigación llevada a cabo. Lo hizo pretendiendo que, al tratarse de una investigación prospectiva, era ilegal y no podía admitirse que la policía hiciese vigilancias en las redes sociales a la búsqueda de actividades delictivas (el tan conocido ciberpatrullaje), como efectivamente sucedió.

La Audiencia Nacional, sin embargo, no compartió esta alegación y fundamentó su negativa como sigue: "*Las fuerzas y cuerpos de Seguridad del Estado tienen como misión entre otras funciones (…) prevenir la comisión de actos delictivos, así como investigar los delitos para descubrir y detener a los presuntos culpables (…). En el ejercicio de estas funciones nada les impide realizar servicios de vigilancia y observación por las calles y por cualquier tipo de lugares públicos, incluidas las redes sociales públicas. Es más, estas actuaciones han resultado esenciales para descubrir delitos en los que las víctimas son las personas más vulnerables, los menores. No es necesaria una denuncia previa para que la policía actúe contra los comportamientos delictivos que observa en un lugar público, sea real o virtual. Lo que no puede hacer cuando actúan de esta forma, que efectivamente puede calificarse de prospectiva, es entrar en un domicilio o intervenir una comunicación privada sea telefónica o telemática, porque lo impiden los derechos fundamentales de inviolabilidad del domicilio, de intimidad o del secreto de las comunicaciones, recogidos en la propia Constitución (…) a modo de ejemplo basta señalar que en el art. 588 quinquies a) (LECrim) permite a la policía judicial obtener y grabar por cualquier medio técnico imágenes de la persona investigada cuando se encuentre en un lugar o espacio público, sin otros requisitos*".

[367] SAN 20/2016, 18 de julio, ARP 2016/781, FD Primero.

De este modo queda claro que el principio de especialidad sólo exige la emisión de mandamientos judiciales para la ejecución de medidas de investigación tecnológica siempre y cuando se proceda para un delito concreto. Los indicios del mismo deben cumplir las dos características señaladas por el Tribunal Constitucional: accesibilidad y control por terceros y base real desconectada de valoraciones personales. Mientras que la prevención, el descubrimiento de delitos o descartar sospechas sin base objetiva, no podrán motivar esta clase de diligencias de investigación limitadoras de los derechos fundamentales del art. 18 CE, por más que la primera y la segunda de esas actividades sí puedan ser llevadas a cabo por los Cuerpos y Fuerzas del Estado en cumplimiento de sus funciones. En esos casos el espacio será público y los entornos virtuales de acceso libre[368].

5.7.2. Principio de idoneidad

El art. 588 bis a núm. 3 LECrim proclama el principio de idoneidad. Según el texto legal servirá este principio para definir el ámbito objetivo, subjetivo y la duración de la medida en virtud de su utilidad.

Una vez determinado que la medida de investigación tecnológica está relacionada con la investigación de un delito concreto, surgen inmediatamente tres interrogantes cuando se trata de aterrizar la concreta medida a aplicar: ¿qué medida va a utilizarse del elenco proporcionado por la reforma de 2015?, ¿quiénes van a ser los sujetos afectados por la misma? y ¿durante cuánto tiempo?. Todo ello, en función de lo que sea más útil para la investigación penal pero, obviamente, sin perder de vista la proporcionalidad que, como luego veremos, es el principio origen de todos los demás y verdadera alma mater que transversalmente los informa a todos.

En palabras de Otamendi Zozaya[369] "*únicamente podrán adoptarse las medidas restrictivas de derechos fundamentales que presumiblemente vayan a ofrecer una*

[368] SANCHIS CRESPO, Carolina; "Principios rectores en la adopción de diligencias limitativas de los derechos reconocidos en el art. 18 CE"; ISSN: 2070-8157, pág. 236
[369] OTAMENDI ZOZAYA, F.: Las últimas reformas de la Ley de Enjuiciamiento Criminal. Una visión práctica tras un año de vigencia, Madrid, 2017, p. 107.

utilidad para la investigación del concreto hecho delictivo que constituye el objeto del proceso, debiendo descartarse aquellas otras que se revelan como inútiles para obtener pruebas o indicios de la comisión del hecho delictivo que se está investigando y de quienes participan en él".

Entendemos que la idoneidad, vista de este modo, tiene estrecha relación con el criterio de utilidad de la actividad probatoria acuñado, en sentido contrario, por la propia Ley de Enjuiciamiento Criminal cuando en su art. 311 afirma que "*El Juez que instruya el sumario practicará las diligencias que le propusieran el Ministerio Fiscal o cualquiera de las partes personadas si no las considera inútiles o perjudiciales*".

La STC 145/2014, 22 de septiembre[370], es ilustrativa de los extremos que deben cubrirse para que la idoneidad se entienda satisfecha. Refiriéndose a la motivación del auto judicial que autoriza la intervención de comunicaciones telefónicas, argumenta el Alto Tribunal que debe explicitarse, en el momento de adopción de la medida: "*(…) todos los elementos indispensables para realizar el juicio de proporcionalidad y para hacer posible su control posterior, en aras del respeto del derecho de defensa del sujeto pasivo de la medida. Por ello, el órgano judicial debe exteriorizar los datos o hechos objetivos que pueden considerarse indicios de la existencia del delito y de la conexión de la persona o personas investigadas con el mismo; indicios que han de ser algo más que simples sospechas (…). Tiene además que determinar con precisión el número o números de teléfono y personas cuyas conversaciones han de ser intervenidas, el tiempo de duración de la intervención, quiénes han de llevarla a cabo y cómo, y los periodos en los que deba darse cuenta al Juez (…). Tales exigencias de motivación se reproducen en las prórrogas y en las nuevas escuchas acordadas a partir de datos obtenidos en una primera intervención, debiendo el Juez conocer los resultados de ésta con carácter previo al acuerdo de prórroga, explicitando las razones que legitiman la continuidad de la restricción del derecho, aunque sea para poner de relieve que persisten las razones anteriores, sin que sea suficiente una remisión tácita o presunta a la inicial*".

Nótese cómo la exigencia de motivación de las causas reclama la fijación del tiempo inicialmente y no decae esta demanda tratándose de las prórrogas. La

[370] STC 145/2014, 22 de septiembre, (RTC 2014, 145), FJ 2.

remisión a las causas iniciales, si éstas persisten, es posible, pero ha de ser expresa.

La idoneidad se resolverá, en cada medida en particular, de una forma particularmente adaptada al caso concreto. El respeto al principio de idoneidad será controlable mediante la exteriorización, en la motivación del auto, de los tres elementos a los que se refiere el art. 588 bis a núm. 3 LECrim. Esto es ámbito objetivo, subjetivo y duración de la medida.Y siempre deberá tenerse presente que el juicio de adecuación a la idoneidad de la medida solicitada debe hacerse ex ante, en el momento de la petición inicial policial como nos recuerda la STS 60/2020, 20 de febrero[371] según la cual: "*(…) el juicio de validez del oficio policial y auto no puede hacerse ex post si se aprehende droga, sino ex ante, a fin de proceder a valorar si se cumplen los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad de la medida. Y, en consecuencia, no procede validar el auto por la circunstancia de que los agentes policiales luego encuentren droga a los investigados, ya que, como efectúa el Tribunal, el juicio de idoneidad y suficiencia debe hacerse ex ante al momento de la petición inicial y valoración de los indicios existentes en la investigación, no siendo suficientes las meras sospechas y/o conjeturas que se explicitan en la sentencia (…) no siendo los argumentos expuestos en el oficio, como antes se ha expuesto con el argumento del Tribunal negando suficiencia a la motivación del auto*".

5.7.3. Principio de excepcionalidad

De la excepcionalidad y la necesidad nos habla el art. 588 bis a en su número 4: "En aplicación de los principios de excepcionalidad y necesidad sólo podrá acordarse la medida:

a) cuando no estén a disposición de la investigación, en atención a sus características, otras medidas menos gravosas para los derechos fundamentales del investigado o encausado e igualmente útiles para el esclarecimiento del hecho o,

[371] STS 60/2020, 20 de febrero, RJ/2020/585, FD Segundo

b) cuando el descubrimiento o la comprobación del hecho investigado, la determinación de su autor o autores, la averiguación de su paradero, o la localización de los efectos del delito se vea gravemente dificultada sin el recurso a esta medida."

Parece desprenderse del modo de formulación de la norma que la excepcionalidad está descrita en el apartado a) mientras que la necesidad lo está en el apartado b). En cualquier caso, ambos principios son las dos caras de una misma moneda, de modo que uno se sustenta en el otro y viceversa[372] por lo que a veces se hace difícil distinguir sus exactos contornos.

La excepcionalidad permite escoger una medida más gravosa frente a otras que lo son menos, por ser la primera más adecuada debido a las concretas circunstancias de la investigación. Esa elección, la de la medida más dañosa, deviene necesaria para que la instrucción avance. Al mismo tiempo, si se acredita como necesario el recurso a una medida más lesiva para que la investigación prospere ello se hace de modo excepcional. La conclusión práctica de lo dicho es que "*el juez debe descartar autorizar medidas restrictivas de investigación tecnológica cuando le consten otras vías menos lesivas para los derechos del investigado, que, con la misma eficacia y similar o incluso menos dificultad, lleven a dar parecida información sobre el extremo o los extremos que se pretendan averiguar*[373]."

Adicionalmente, sobre la aplicación del principio de excepcionalidad nos hablan multitud de sentencias, de entre ellas destacamos la STS 982/2016, 11 de enero de 201724, en la que se examina la observancia de este principio en la autorización de una intervención de comunicaciones telefónicas: "*De la nota de excepcionalidad se deriva que la intervención telefónica no supone un medio normal de investigación, sino excepcional en la medida que supone el sacrificio de un derecho fundamental de la persona, por lo que su uso debe efectuarse con carácter limitado, ello supone que ni es tolerable la petición sistemática en sede judicial de tal autorización, ni menos se debe conceder de forma rutinaria. Ciertamente en la mayoría de los*

[372] Nótese que el propio legislador los agrupa en el mismo número reconociendo de alguna manera su carácter complementario.
[373] VELASCO NUÑEZ, E., Delitos tecnológicos…, cit., p. 69

supuestos de petición se estará en los umbrales de la investigación judicial -normalmente tal petición será la cabeza de las correspondientes diligencias previas-, pero en todo caso debe acreditarse una previa y suficiente investigación policial que para avanzar necesita, por las dificultades del caso, de la intervención telefónica, por ello la nota de la excepcionalidad, se completa con las de idoneidad y necesidad y subsidiariedad formando un todo inseparable, que actúa como valladar ante el riesgo de expansión que suele tener todo lo excepcional, riesgo sobre el que esta Sala ha llamado la atención varias veces. (…)". Idoneidad porque este medio aparezca adecuado para los fines de la instrucción, necesidad porque no existe otro medio de investigación menos invasivo, y subsidiariedad porque ya se han agotado otros medios de investigación. Son garantías y cautelas para impedir que las intervenciones se conviertan en fuente de abusos de poder de la mano de estas modernas técnicas que, sí es claro que permiten avanzar investigatorias, también suponen nuevos riesgos para los derechos de las personas.

Como vemos, según el Tribunal Supremo Español, son incompatibles con la excepcionalidad, por su carácter extraordinario, las peticiones sistemáticas, las concesiones rutinarias y la solicitud de esta clase de medidas invasivas sin una previa y suficiente investigación policial. El Tribunal pone asimismo de manifiesto la estrecha relación entre los principios rectores que estamos analizando.

Entendemos que la doctrina también se ha referido a este principio, años antes de su formulación expresa en la Ley de Enjuiciamiento Criminal Española, cuando hablaba de la subsidiariedad como un subprincipio del principio constitucional de prohibición de exceso que tiende a la optimización del grado de eficacia de los derechos individuales frente a las limitaciones que pudieran imponer en su ejercicio los poderes públicos. Obliga a los órganos del Estado a comparar las medidas restrictivas aplicables que sean suficientemente aptas para la satisfacción del fin perseguido y a elegir, finalmente, aquella que sea menos lesiva para los derechos de los ciudadanos[374].

[374] GONZÁLEZ-CUÉLLAR SERRANO, N.: "El principio de proporcionalidad en el Derecho procesal español", Cuadernos de Derecho Público, núm. 5 (septiembre-diciembre 1998), p. 206. El autor hacía equivaler este principio al de necesidad.

5.7.4. Principio de necesidad

Sobre el principio de necesidad aparece también en multitud de sentencias. De ellas seleccionamos dos. En la primera, la STS 391/2016, 6 de mayo[375], nos situamos ante un supuesto en el que el principio de necesidad no se cumplió. El recurrente cuestiona la nulidad de las intervenciones telefónicas que la Audiencia decretó apoyada en dos argumentos: el hecho de considerar que no se cumplió en la autorización judicial de la diligencia el principio de necesidad, toda vez que la solicitud policial se formuló sin haber agotado previamente la práctica de otros medios de investigación que evidencien lo imprescindible de la realización de las "escuchas", así como que tampoco la resolución autorizante motivaba con suficiencia las razones por las que se produjo el cambio de líneas telefónicas, objeto de investigación, correspondientes a otros titulares distintos del sospechoso inicial.

El Tribunal Supremo argumenta: "*Si bien le asiste plenamente la razón al Fiscal en cuanto a la existencia de constatada necesidad de la injerencia en el derecho fundamental al secreto de las comunicaciones de la autorización inicial, subsiste, sin embargo, el segundo de los argumentos utilizados por la Audiencia pues, en efecto, cuando se interesa que se extienda la intervención a otras líneas telefónicas correspondientes a distintas personas, no se explica en ningún momento, ni por la Policía al interesarlo ni por el Instructor al acceder a esa solicitud, las razones por las cuales las sospechas se extendían a estos nuevos titulares. Y es que no nos hallamos ante el supuesto, al que al parecer nos quiere remitir el Fiscal, de aquellas otras ocasiones en las que resulta indiferente la titularidad de los equipos participantes en las comunicaciones objeto de intervención que, en efecto, es circunstancia irrelevante en orden a la protección del derecho invadido, sino que, en este caso, de lo que se trata realmente, como el resultado de la investigación a la postre evidenció, era extender a otros sujetos la investigación misma, lo que, obviamente, no puede hacerse sin la suficiente justificación para ello*".

Observemos cómo, en primer lugar, aparecen nuevamente amalgamados excepcionalidad y necesidad en el primero de los argumentos de la Audiencia que se cifraba en que la solicitud policial se formuló sin haber agotado previamente la

[375] STS 391/2016, 6 de mayo, RJ 2016/1969, FD Primero.

práctica de otros medios de investigación que evidencian lo imprescindible de la realización de las intervenciones telefónicas.

El segundo de ellos, el referido a que el auto no motivaba con suficiencia las razones por las que se produjo un cambio en las líneas telefónicas investigadas, sí nos parece encuadrable en el diseño legal del principio de necesidad. Este cambio no era solo de líneas, sino también de personas titulares de las mismas, por lo que requería una adecuada motivación. De no haberse ampliado el objeto de la investigación a esas otras líneas, la investigación se vería gravemente dificultada, como expresa el art. 588 bis a núm. 4 b LECrim. Al no observarse el principio de necesidad y constatar así el Tribunal Supremo, las pruebas de este modo obtenidas no son valorables y se frustra el trabajo policial.

En la segunda de las sentencias seleccionadas, la STS 646/2012, 13 de julio[376], sí se estimó satisfecho el principio de necesidad. "*La parte recurrente hace especial hincapié en la falta del requisito de la necesidad de la medida, y alega que había que profundizar previamente en la investigación sobre los bienes patrimoniales de Fermín. Sin embargo, tal como se razona en la sentencia impugnada, una vez que los encargados de la pesquisa habían detectado que Marco Antonio, ahora recurrente, residía temporadas fuera de España (en Holanda) y que Fermín era, en principio, su representante permanente en el territorio español, pues vivía de forma estable en la costa malagueña, la progresión de la investigación se hacía muy difícil sin acceder a lo que hablaban entre ellos*". Nuevamente aquí se vincula el principio de necesidad con la medida de investigación más adecuada para hacer progresar la investigación, con la diferencia, respecto al caso tratado en la sentencia anterior, de que aquí sí se motivó suficientemente y por tanto se respetó el principio rector.

[376] STS 646/2012, 13 de julio, RJ 2012/11347, FJ Segundo

5.7.5. Principio de proporcionalidad

A la proporcionalidad dedica el art. 588 bis a LECrim el quinto y último punto. Según este precepto, las medidas de investigación tecnológica[377] solo se reputarán proporcionadas cuando, tomadas en consideración todas las circunstancias del caso, el sacrificio de los derechos e intereses afectados no sea superior al beneficio que de su adopción resulte para el interés público y de terceros. Para la ponderación de los intereses en conflicto, la valoración del interés público se basará en la gravedad del hecho, su trascendencia social o el ámbito tecnológico de producción, la intensidad de los indicios existentes y la relevancia del resultado perseguido con la restricción del derecho.

A primera vista este número del artículo parece el más extenso, tanto en su formulación como en el alcance de su significado. Es lógico que así sea. Como hemos adelantado anteriormente, este principio de proporcionalidad es la columna vertebral del resto de principios. Es el principio marco en el que todos los demás encuentran cabida[378].

La STC 207/1996, 16 de diciembre[379] -muy distante en el tiempo de la reforma de la LECrim de 2015-, ya vislumbró esta idiosincrasia del principio de proporcionalidad. Lo hizo permitiendo distinguir entre la proporcionalidad en sentido amplio y la proporcionalidad en sentido estricto. La primera de ellas daría cobijo al resto de principios rectores, mientras que la segunda añadiría una nota específica configuradora de la esencia de la proporcionalidad.

Recordando la doctrina sobre este principio, resumía así el Tribunal los requisitos que debía cumplir la medida de investigación para ajustarse a la proporcionalidad: "*(…) que la medida limitativa del derecho fundamental esté*

[377] Nótese que el artículo habla literalmente de las "las medidas de investigación reguladas en este capítulo". Está claro que no se limita a este capítulo, sino que alcanza hasta el capítulo IX. Y, en cualquier caso, la referencia quedaría corta porque estos principios rectores habrán de regir la aplicación no solo de las medidas de investigación tecnológica, sino también la de todas aquellas medidas que supongan una limitación de los derechos fundamentales del investigado.

[378] Sobre el principio de proporcionalidad existen variadas aportaciones doctrinales. Destacamos dos que la abordan monográficamente. González-Cuéllar Serrano, N.: "El principio de proporcionalidad en el Derecho procesal español", cit. y Pedraz Penalva, E. y Ortega Benito, V.: "El principio de proporcionalidad y su configuración en la jurisprudencia del Tribunal Constitucional y literatura especializada alemanas", Revista del Poder Judicial, núm. 17, marzo 1990, pp. 1-27

[379] STC 207/1996, 16 de diciembre, (RTC 1996, 207). Las citas de esta sentencia son todas al FJ 4.

prevista por la Ley, que sea adoptada mediante resolución judicial especialmente motivada, y que sea idónea, necesaria y proporcionada en relación con un fin constitucionalmente legítimo". Líneas después identificaba este fin como "el interés público propio de la investigación de un delito, y, más en concreto, la determinación de hechos relevantes para el proceso penal (…)".

El Tribunal reconoce como exigencia común y constante para la constitucionalidad de cualquier medida restrictiva de derechos fundamentales, la estricta observancia del principio de proporcionalidad. Y describe con más detalle los requisitos anteriormente mencionados condensándolos en tres: "*(…) para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres siguientes requisitos o condiciones: si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto)*".

De la doctrina que se establece en esta sentencia podemos colegir, como adelantábamos, una proporcionalidad en sentido amplio y otra en sentido estricto. En la primera se englobarían los principios examinados hasta ahora: la legalidad, la especialidad, la idoneidad, la excepcionalidad y la necesidad. Esto es así porque todos contemplan transversalmente una dosis de proporcionalidad adaptada a las concretas exigencias de cada uno. Sin embargo, la esencia misma de la proporcionalidad es la denominada por el Tribunal "proporcionalidad en sentido estricto" y consiste en analizar si de la adopción de la medida se derivan "más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto". El interés general será aquí el de la investigación penal y los bienes o valores en conflicto, los intereses y derechos fundamentales del investigado.

La cuestión que surge a continuación es cómo saber cuándo el fiel de la balanza se inclina a favor del interés general de la investigación penal o en defensa

de los intereses y derechos fundamentales particulares del investigado. Será esa, sin duda, una pregunta que tendrá que resolver el juez de instrucción atendiendo a las peculiaridades de cada caso concreto y sobre la que no pueden aventurarse juicios previos. Sí pueden, sin embargo, plantearse algunos parámetros que sirvan de guía. Es esto precisamente lo que hace el art. 588 bis a núm. 5 LECrim in fine cuando dice que "*para la ponderación de los intereses en conflicto, la valoración del interés público se basará en la gravedad del hecho, su trascendencia social o el ámbito tecnológico de producción, la intensidad de los indicios existentes y la relevancia del resultado perseguido con la restricción del derecho*".

Como vemos, se enumeran hasta cuatro parámetros. A saber: a) la gravedad del hecho; b) su trascendencia social o el ámbito tecnológico de producción; c) la intensidad de los indicios existentes y d) la relevancia del resultado perseguido con la restricción del derecho.

El primero de ellos parece el más evidente de todos y el más fácilmente constatable. No obstante, esta característica de la gravedad exige ser matizada. El delito grave no es solo el que a efectos penal tenga esa cualidad, sino también el que, por su trascendencia social, pueda ser así considerado. En este sentido la Audiencia Provincial de Toledo 137/2015, 5 de noviembre[380], se refiere a ello conectando la gravedad del hecho con el segundo de los parámetros de la proporcionalidad en sentido estricto, esto es, la trascendencia social. Así, razona la Audiencia que: "*La proporcionalidad tiene como consecuencia que este medio excepcional de investigación requiere una gravedad acorde y proporcionada a los delitos a investigar. Señala la Jurisprudencia que el interés del Estado y la sociedad en la persecución y descubrimiento de los hechos delictivos es directamente proporcional a la gravedad de estos, por ello sólo en relación a la investigación de delitos graves será adecuado el sacrificio de los derechos fundamentales para facilitar su descubrimiento pues el juicio de proporcionalidad de los intereses en conflicto desaparecería si por delitos menores se generalizase este medio excepcional de investigación con generalizado quebranto de derechos fundamentales. Frente a otras legislaciones que establecen el catálogo de delitos*

[380] Audiencia Provincial de Toledo 137/2015, 5 de noviembre, JUR 2015/302509, FD Quinto.

para cuya investigación está previsto este medio excepcional, la legislación española vigente en el momento de iniciarse esta causa y en este momento actual guarda silencio que se interpreta por la Jurisprudencia como exigencia de que se esté en la investigación de hechos delictivos graves (…) También es Jurisprudencia reiterada la que determina que la gravedad del delito no se valora solo atendiendo a la previsión legal para el mismo de una pena privativa de libertad grave, sino también apreciar la trascendencia social del delito que se trata de investigar (…). La trascendencia social tiene relación con la alarma social (…) y se valora la misma sobre la base de que sea un delito que se venga cometiendo habitualmente (…). Es más, la alarma social hace referencia al sentimiento social de inseguridad en lo más básico dada la reiteración de estos delitos y esto es socialmente trascendental".

Respecto al concepto de delito grave, en relación a la proporcionalidad, parecía que la resolución de la cuestión prejudicial C-207/2016, planteada por la Audiencia Provincial de Tarragona[381], iba a resolver las dudas acerca de lo que debía entenderse por tal, a la luz del derecho europeo. El 3 de mayo de 2018 el Abogado General presentó sus Conclusiones a la petición de decisión prejudicial. En su opinión, formulada en el punto 105, "*aunque la pena tiene una importancia considerable, otros factores objetivos deben asimismo tenerse en cuenta (…). Concretamente se trata, por un lado, del contexto en el que se inscribe el delito cuya comisión se imputa –si la conducta delictiva es de carácter doloso, concurren circunstancias agravantes o el autor es reincidente –, por otro lado, de la importancia de los bienes jurídicos de la sociedad que han podido resultar lesionados por el autor del delito y la naturaleza o la magnitud de los daños sufridos por la víctima y, por último de la gradación de las penas en general en el Estado miembro de que se trate. A mi juicio procede calificar en su caso un delito de "grave", en el sentido de la jurisprudencia del Tribunal de Justicia, a partir de este conjunto de criterios de apreciación, alternativos y no exhaustivos*".

El procedimiento principal que dio lugar al planteamiento de la citada cuestión prejudicial, se inició con una denuncia ante la Policía por un robo con violencia

[381] Respecto a la interposición de esta Cuestión prejudicial véase Bahamonde Blanco, M., "Medidas de investigación tecnológica a la luz de los derechos fundamentales, una cuestión pendiente", Diario La Ley, nº 9160, Sección Tribuna, 16 de marzo de 2018, pp. 1-6.

cometido el 16 de febrero de 2015. El 27 de febrero del mismo año la Policía Judicial presentó un oficio ante el Juez instructor solicitando que se ordenase a diversos proveedores de servicios de comunicaciones electrónicas la transmisión de los números de teléfonos activados, desde el 16 de febrero hasta el 27 de febrero de 2015, con el código relativo a la identidad internacional del equipo móvil (IMEI) del teléfono móvil sustraído, así como los datos personales o de filiación de los titulares o usuarios de los números de teléfono correspondientes a las tarjetas SIM activadas con dicho código, como su nombre, apellidos, y en su caso, dirección.

El juez instructor denegó la diligencia solicitada pues entendió que la Ley 25/2007 de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, limitaba la cesión de los datos conservados por las operadoras de telefonía a los delitos graves y con arreglo al Código Penal español el delito en cuestión -robo con violencia- no pertenecía a esa categoría. El Ministerio Fiscal interpuso recurso de apelación contra dicho auto y posteriormente el juez planteó la cuestión prejudicial expuesta en dos fundamentales preguntas:

> 1) La suficiente gravedad de los delitos como criterio que justifica la injerencia en los derechos fundamentales reconocidos en los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea ¿puede identificarse únicamente en atención a la pena que pueda imponerse al delito que se investiga o es necesario, además, identificar en la conducta delictiva particulares niveles de lesividad para bienes jurídicos individuales y/o colectivos?
>
> 2) En su caso, la determinación de la gravedad del delito atendiendo a la pena imponible ¿sería compatible con una previsión general de límite de tres años de prisión? ¿Cuál debería ser ese umbral mínimo?

Parecía, viendo el planteamiento de las cuestiones prejudiciales, que el Tribunal aclararía cuál era el estándar de gravedad del delito que permitiría una injerencia en los derechos a la intimidad y a la vida privada. Y, caso de identificarse estrictamente con un criterio de gravedad penológica, se determinaría si los tres años eran un umbral mínimo aceptable o, en su caso, dónde situarlo. Sin embargo,

el Tribunal, aunque dio en su sentencia de 2 de octubre de 2018 una solución al caso planteado, no contestó estrictamente las cuestiones formuladas.

En efecto, el Tribunal parte de una distinción ente injerencias leves e injerencias graves en los derechos fundamentales consagrados en los arts. 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea[382]. Considera que los datos referidos únicamente al número de teléfono correspondiente a la tarjeta SIM, así como los datos personales o de filiación de los titulares de dichas tarjetas, como su nombre apellidos y, en su caso, dirección, no pueden calificarse de injerencia grave. Son datos estos que no permiten extraer conclusiones precisas sobre la vida privada de las personas cuyos datos se ven afectados y por tanto no presentan una gravedad tal que dicho acceso deba limitarse, en el ámbito de la prevención, investigación, descubrimiento y persecución de delitos, a la lucha contra la delincuencia grave.

En cambio, los datos relativos a las comunicaciones efectuadas en el teléfono, a su localización, fecha, hora y duración de las llamadas, destinatarios de las comunicaciones efectuadas con la tarjeta SIM en cuestión o la frecuencia de estas con determinadas personas cotejados con los anteriores datos, sí permitirían extraer esas conclusiones a las que nos referíamos. Parece desprenderse de la sentencia que, en caso de delincuencia no grave, tales injerencias no serían soportables.

Con la resolución de esta cuestión prejudicial el Tribunal ha determinado la compatibilidad de nuestro ordenamiento con el derecho de la Unión, en el caso de estas injerencias leves, pero queda por saber de una manera precisa si esas otras injerencias graves -que la normativa actual sobre investigación tecnológica española permite- se ajustan al derecho de la Unión.

En cualquier caso, junto a la interpretación de la gravedad del delito bajo un criterio no penal, siempre estará la anudada a delitos graves. Así lo indica la STS

[382] Artículo 7. Respeto de la vida privada y familiar Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones. Artículo 8. Protección de datos de carácter personal 1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan. 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación. 3. El respeto de estas normas quedará sujeto al control de una autoridad independiente.

626/2019, 18 diciembre[383]: "(…) resulta evidente que dada la gravedad de los hechos y la amplitud de personas que estaban interviniendo, conforme se detectó resultaba clara la proporcionalidad de la injerencia y su prórroga, a fin de poder detectar y comprobar el alcance de los hechos de tanta gravedad que se estaban produciendo y detectar quiénes lo estaban llevando a cabo, a fin de cerrar el círculo de los que estaban llevando a cabo estos actos ilícitos en lugar de velar por el cumplimiento de la Ley. Resulta evidentemente proporcional adoptar las medidas judiciales de injerencia cuando se trata de delitos de corrupción en donde las autoridades públicas y los funcionarios públicos en lugar de velar por cumplir su función de protección y tutela de los intereses públicos se aprovechan de su condición de la que se prevalen para cometer estos hechos delictivos amparados en su poder, lo que les permite una facilitación del delito, y en algunos casos la dificultad de su descubrimiento, salvo que en los delitos de cohecho, los que son sobornados pongan en conocimiento de la autoridad lo ocurrido para depurar las responsabilidades penales por los mismos. En esta tesitura la proporcionalidad de la medida de injerencia y de las prórrogas resulta evidente".

El segundo de los parámetros para evaluar la proporcionalidad es la trascendencia social del delito investigado que se hace equivaler en el precepto al denominado ámbito tecnológico de producción. Esta asimilación llevada a cabo por el legislador constata la tendencia de transformación digital a la que nos referíamos en apartados precedentes. Actualmente la trascendencia social del delito se hace notar tanto en el mundo físico como en el mundo virtual. Por eso ha hecho bien el legislador en equipararlos, puesto que si el ámbito de producción del delito es de carácter tecnológico la trascendencia del mismo está prácticamente asegurada.

En tercer lugar, la intensidad de los indicios existentes se revela también como un buen cuantificador del principio de proporcionalidad. Cuanta más fuerza incriminatoria posean, más se fortalecerá la línea de investigación que se dirija a adoptar una herramienta tecnológica en concreto.

A un nivel más local, en Argentina, en relación a la discusión sobre la afectación a la intimidad que producía la implementación de un sistema

[383] STS 626/2019, 18 diciembre, RJ/2019/5423, FD Séptimo.

videovigilancia con detección biométrica (en Ciudad Autónoma de Buenos Aires), dicho sistema fue cuestionado, entre otros, por el relator especial sobre el derecho a la privacidad, Joe Cannataci[384] sostuvo que "no veo la proporcionalidad de instalar una tecnología con graves implicaciones para la privacidad para buscar en una lista de 46.000 personas que actualmente incluye a menores y delitos no graves...". Es decir, la implementación de dicha medida no satisface el principio de proporcionalidad que debe tener toda interferencia a un derecho fundamental.[385]

5.8. Medidas que no requieren autorización judicial

5.8.1. Identificación de dirección IP

Normalmente en la mayoría de las investigaciones, nos encontraremos con la necesidad de determinar información relacionada a una dirección IP. Brevemente, diremos que la dirección IP[386] es una etiqueta numérica que identifica a una interfaz (elemento de comunicación/conexión) de un dispositivo (ordenador, móvil, pda, ipad, televisión, ebook, consola de videojuegos) dentro de una red que utiliza el protocolo IP (Internet Protocol). Las direcciones IP son asignadas por los ISP (Internet service provider), compañías proveedoras de acceso a Internet (Telefónica, Telecom, Claro).

Comenzaremos a desandar la respuesta a la pregunta, partiendo del principio básico acerca de que "no se precisa autorización judicial para conseguir lo que es público"[387]. El Tribunal Supremo Español considera que estos datos no se encuentran protegidos ni por el art. 18.1 CE, ni por el art. 18.3 CE (STS 1299/2011

[384] ONU, Declaración del Relator Especial sobre el derecho a la privacidad tras visitar Argentina; 17/5/2019; disponible en www.onu.org.ar/declaracion-del-relator-especial-sobre-el-derecho-a-la-privacidad-tras-visitar-argentina/

[385] FERREYRA, Eduardo; "El ojo blindado. Una perspectiva de derechos fundamentales sobre el uso de tecnología de reconocimiento facial por parte de fuerzas de seguridad"; publicado en el Libro Sistema Penal e Informática, Volumen 3; de Dirección de Marcelo Riquert y Coordinación por Carlos Christian Sueiro. Editorial Hammurabi.

[386] En gran parte de Latinoamérica, las direcciones IP utilizadas son versión 4 del protocolo IP, que consta de cuatro números separados por puntos, y cada número con un valor que oscila de 0 a 255. Se está implantando la versión 6 del protocolo IP, que consta de 16 números separados por dos puntos y con estructura diferente al anterior protocolo. "IPV6 Aspectos Legales del nuevo protocolo de Internet". Euro6ix. Comisión Europea. http:// ipv6tf.org.

[387] Jurisprudencia STS 739/2008, de 12 de noviembre

de 17 de noviembre; STS 292/2008, de 28 de mayo; y STS 776/2008, de 18 de noviembre), por lo que la Policía o Fuerza de Seguridad a cargo de la investigación se encuentra habilitada para obtener la identificación IP sin que sea necesario obtener autorización judicial.

Ahora bien, es preciso tener en cuenta que la jurisprudencia distingue por un lado, los casos de rastreo policial del espacio público, y por otro los supuestos en los que para acceder a una información sobre IP es necesario oficiar a una operadora ISP. En este último supuesto, sí debe considerarse necesario obtener autorización judicial conforme a las previsiones del art. 588 ter k de la LECrim y de la Ley 25/2007, de conservación de datos (SSTS 292/2008, de 28 de mayo, 236/2008, de 9 de mayo, 680/2010, de 14 de julio). Aquí la exigencia deriva del mandato legal pese a que el dato no pueda cobijarse bajo el manto protector del secreto de las comunicaciones (ya que técnicamente, son datos de abonado).

Es decir, confirmamos que es preciso acudir a la autorización del juez competente para desvelar la identidad de la terminal, teléfono o titular del contrato de un determinado IP, en salvaguarda del derecho a la intimidad personal (habeas data).

Volviendo al primer caso, los rastreos policiales para localizar direcciones IP pueden realizarse sin necesidad de autorización judicial ya que no se trata de datos confidenciales preservados del conocimiento público. La barrera entre lo público (la Red), en donde la policía y cualquier particular pueden rastrear los vestigios dejados por el atacante informático, y lo privadamente protegido, donde no cabe inmiscuirse legalmente salvo que lo permita el afectado o lo autorice un juez.

Ahora bien, cabe distinguir que es lo que se está considerando el rastreo policial que accede a dichos registros. En este sentido, es de especial interés la STS 1299/2011 de 17 de noviembre en la que se establece que "*Los rastreos que realiza el equipo de delitos telemáticos de la Guardia Civil en Internet tienen por objeto desenmascarar la identidad críptica de los IP que habían accedido a los "hash" que contenían pornografía infantil. El acceso a dicha información, calificada de ilegítima o irregular, puede efectuarla cualquier usuario. No se precisa autorización judicial para conseguir lo que es público y el propio usuario de la red es quien lo ha introducido*

en la misma. La huella de la entrada queda registrada siempre y ello lo sabe el interesado".

En el mismo sentido, prosigue la STS 680/2010, de 14 de julio, al tratar de los rastreos informáticos policiales, "*la STS 292/2008, de 28 de mayo, ya declaró que cuando la comunicación a través de la Red se establece mediante un programa P2P, como en el EMULE o EDONKEY, al que puede acceder cualquier usuario de aquella, el operador asume que muchos de los datos que incorpora a la Red pasen a ser de público conocimiento para cualquier usuario de internet, como, por ejemplo el IP, es decir, la huella de la entrada al programa, que queda registrada siempre. Y fue este dato, el IP del acusado, el que obtuvo la Guardia Civil en su rastreo de programas de contenido pedófilo, dato que -conviene repetir y subrayar- era público al haberlo introducido en la Red el propio usuario al utilizar el programa P2P. Por ello, no se precisa autorización judicial para conocer lo que es público, y esos datos legítimamente obtenidos por la Guardia Civil en cumplimiento de su obligación de persecución del delito y detención de los delincuentes, no se encontraban protegidos por el art. 18.3 CE.*"

Como se puede observar, los casos que analiza la jurisprudencia en relación al acceso a la dirección IP (u otros datos similares) son en realidad, información que ha quedado almacenada en un registro determinado, y que por lo tanto, sería información accesible sin necesidad de autorización judicial.

Ahora bien, nos queda un caso más complejo por analizar: la posibilidad de interactuar técnicamente con el sistema o cuenta bajo investigación, a fin de obtener estos mismos datos (dirección IP, sistema operativo, dispositivo utilizado, etc.). Es decir, aquí ya no se trata de una acción o hecho pasado, donde esos registros han quedado plasmados (como una huella que ha quedado sobre el barro), sino que se trata de un nuevo hecho, provocado por la Fuerza de Seguridad que ejecuta la medida, a fin de poder establecer e identificar dichas huellas (en el mismo ejemplo, sería como tener la posibilidad de hacer caminar a la persona sospechada en un nuevo escenario preparado con barrio, a fin de lograr que las huellas de su calzado queden registradas para un posterior análisis investigativo).

Este tipo de situaciones se da con la medida (que veremos con mayor detalle técnico más adelante) denominada “Identificación de dispositivo mediante captación de información de sistema”, donde básicamente esta técnica consiste en la recolección, procesamiento y análisis de un conjunto de información que expone un dispositivo o sistema determinado al conectarse a un servidor controlado por el investigador.

Entre la información que puede ser captada de la interacción con un sistema o dispositivo, podemos mencionar el sistema operativo utilizado, su versión, navegador de internet utilizado, plugins instalados, fuentes instaladas en dicho sistema, resolución de pantalla utilizada por el dispositivo, dirección IP pública utilizada por la conexión a internet, modelo del dispositivo celular utilizado (en el caso que la conexión sea realizada desde un celular) hasta incluso, en algunos casos, la ubicación geográfica de la persona conectada.

Del conjunto de todos los datos que se puedan recolectar del dispositivo de interés, usualmente se procede a realizar un agrupamiento de este conjunto de datos, generando una “huella digital” del dispositivo, que podrá ser de utilidad para la investigación en curso.

La clave es que, en determinados casos, para poder obtener esta información de interés para la investigación es necesario interactuar con dicho sistema (o persona que manipula el sistema). Afirmamos que es en determinados casos toda vez que existen herramientas como “Shodan”[388], que permiten realizar escaneos externos, determinando por ejemplo, conexiones abiertas, sistemas instalados, versiones, vulnerabilidades existentes, etc. Esta información, puede ser consultada sin necesitar una interacción con una persona, sino que son escaneos automatizados (robots) que van consultando información sobre lo que existe sobre la dirección IP de interés, y van listando lo que es posible obtener.

[388] Shodan.io

5.8.2. Identificación de IMEI, IMSI y MAC.

Con el término IMSI se hace referencia a un código de identificación único para cada línea de telefonía móvil integrada en la tarjeta SIM (Subscriber Identity Module) que permite la identificación del abonado a través de las redes GSM y UMTS.

A modo de ejemplo, es posible obtener el IMSI de un teléfono móvil mediante un aparato especial que simula el comportamiento de la red GSM y con el que inicia un diálogo de forma equivalente al que se sigue en la infraestructura de red de un operador móvil cuando se enciende el móvil o se cambia de célula de cobertura. Para ello es preciso que el aparato se utilice en las proximidades del teléfono que se desea investigar.

Por su parte, el término IMEI es un código pregrabado en los teléfonos móviles que identifica al aparato unívocamente a nivel mundial y se transmite por el móvil a la red de telefonía al conectarse a ésta. Es el equivalente al número MAC, cuando nos referimos a móviles, pues identifica ese número de serie al equipo.

El término MAC es un identificador de 48 bits que corresponde de forma única a una tarjeta o dispositivo de red, también conocida como dirección física y es única para cada dispositivo. Las direcciones MAC son únicas a nivel mundial y constituyen una huella digital que permite determinar desde qué dispositivo de red se ha emitido un determinado paquete de datos.

Sin embargo, aquí está la clave: tanto el MAC, el IMEI y el IMSI carecen de capacidad de información sobre la identidad del usuario, teniendo valor únicamente si se asocia a otros datos en poder de las operadoras.

Es decir, la captación de tales números a efectos de investigación penal es posible mediante un escaneado o barrido realizado a través de instrumentos electrónicos que detectan aquellos siempre que se actúe en un determinado radio de acción en el que se encuentra el terminal. Su captación se realiza como consecuencia de un seguimiento dirigido específicamente frente a un individuo o individuos determinados.

Con posterioridad a la captación, una vez obtenido el correspondiente código identificativo, es necesaria la obtención del número comercial del teléfono, en posesión de la prestadora del servicio de telecomunicación. Ni el MAC, ni el IMSI, ni el IMEI por sí solos, son datos integrables en el concepto de comunicación.

En cuanto a la obtención de los IMSI, el Tribunal Superior Español refrenda la legitimidad de que sea la propia policía quien los obtenga por sus medios técnicos en la medida que con ellos se desconoce incluso el número telefónico concernido y las llamadas que pudieran recibirse y efectuarse (STS 1115/2011, de 17 de noviembre; STS 79/2011, de 15 de febrero; STS 249/2008, de 20 de mayo; STS 776/2008, de 18 de noviembre).

La utilización de herramientas electrónicas que rastrean el espectro radioeléctrico forzando a los dispositivos cercanos a generar un diálogo automático con la herramienta a través de la que facilitan a ésta las asignaciones numéricas que se corresponden con los números IMEI o IMSI se encontraba carente de una cobertura legal; más allá de una consolidada jurisprudencia del Tribunal Supremo que sistemáticamente validaba tal forma de investigación, siempre que a través de este vía no se accediera a lo que eran auténticos datos de tráfico de comunicaciones.

La LECrim, de acuerdo con la jurisprudencia, regula la identificación de los terminales mediante captación de códigos de identificación como el IMSI o el IMEI, habilitando a los Cuerpos Policiales a la utilización de artificios técnicos que permitan su obtención, sin necesidad de autorización judicial (artículo 588 ter l LECrim).

Ahora bien, aunque la LECrim no hace referencia expresa al término MAC, como sucede con el IMSI e IMEI debería entenderse incluido también en la fórmula abierta y amplia utilizada en este precepto. De la misma forma, entendemos que sucede con la dirección IP, analizada previamente (entendiendo que no forma parte de datos de tráfico ni obviamente, de datos de contenido).

Ahora bien, tanto con el IMSI como con el IMEI o MAC se dispone de información suficiente como para poder solicitar la identificación por el operador de los números de teléfono que corresponden a tales datos, o la correspondiente

intervención de las comunicaciones. Sin embargo, en España no puede la Policía solicitar directamente tal información de las operadoras toda vez que la Ley 25/2007, de 18 de octubre, de Conservación de Datos de las Comunicaciones Electrónicas, incluye en el art. 3.1 dentro de su ámbito de aplicación los datos IMSI, IMEI y MAC para cuya cesión resulta exigible la misma regla impuesta para el resto de los datos a los que se refiere, esto es, la preceptiva autorización judicial.

Entendemos entonces que este tipo de técnica se trataría de un auténtico acto previo a una solicitud de intervención de comunicaciones, aunque la posibilidad de utilización de tal estrategia, quedaría limitada a aquellos supuestos en los que pudiera ser procedente, en términos de tipos penales susceptibles de permitir en abstracto una injerencia.

La norma española[389], sin embargo, se muestra más ambiciosa y abre las puertas a otras posibilidades de indagación, de acuerdo con el estado de la tecnología. La barrera infranqueable para estas vías de prospección se debe establecer en la prohibición de que el acceso a la información tenga lugar mediante cualquier forma o vía de interceptación que la extraiga de comunicaciones en curso, sometidos a la inexcusable previa autorización judicial de interceptación; o datos relativos a comunicaciones ya consumados, sometidos a la disciplina del art. 588 bis c.

Es decir, con dicha normativa no solamente no se necesita autorización judicial para obtener el IMSI o IMEI, sino, en general, de cualquier medio técnico que, de acuerdo con el estado de la tecnología, sea apto para identificar el equipo de comunicación utilizado o la tarjeta utilizada para acceder a la red de telecomunicaciones.

[389] Ley de Enjuiciamiento Criminal, Artículo 588 ter l. "*Identificación de los terminales mediante captación de códigos de identificación del aparato o de sus componentes. 1. Siempre que en el marco de una investigación no hubiera sido posible obtener un determinado número de abonado y este resulte indispensable a los fines de la investigación, los agentes de Policía Judicial podrán valerse de artificios técnicos que permitan acceder al conocimiento de los códigos de identificación o etiquetas técnicas del aparato de telecomunicación o de alguno de sus componentes, tales como la numeración IMSI o IMEI y, en general, de cualquier medio técnico que, de acuerdo con el estado de la tecnología, sea apto para identificar el equipo de comunicación utilizado o la tarjeta utilizada para acceder a la red de telecomunicaciones.*"

5.8.3. Identificación de titulares o terminales o dispositivos de conectividad.

El artículo 41.1 de la Ley General de Telecomunicaciones establece la obligación de los operadores de garantizar los niveles de protección de datos exigidos por la LO 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD).

En igual sentido, el artículo 48 de la citada Ley de Telecomunicaciones relaciona los derechos de privacidad de los abonados, y concretamente en su apartado 3 se refiere a la protección de datos y a la privacidad en relación con las guías de abonados.

De conformidad con lo dispuesto en el artículo 11 de la LOPD los datos de carácter personal sólo podrán ser comunicados a terceros previo consentimiento del interesado, si bien no es preciso dicho consentimiento en los supuestos exceptuados en el mismo artículo, uno de los cuales es el siguiente:

Art. 11.2 f) Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces y Tribunales o el Tribunal de Cuentas en el ejercicio de las funciones que tiene atribuidas.

Por tanto, la autoridad judicial puede acceder a la información sobre abonados, en todo caso, en el curso de una investigación criminal de acuerdo con el artículo 18 CE y con la normativa específica antes mencionada.

El Ministerio Fiscal podrá hacerlo inicialmente con base a lo dispuesto en el artículo 11.2 f) de la LOPD, antes citado, salvo que dicha información se encuentre vinculada al secreto de las comunicaciones o cuando se necesite dicha autorización judicial.

En lo que concierne a las Fuerzas y Cuerpos de Seguridad, en España tanto el Tribunal Constitucional como el Tribunal Supremo tradicionalmente han entendido que cuando el acceso a esa información no afecte al secreto de las comunicaciones, sino únicamente al derecho a la intimidad personal, y concurran circunstancias de

urgencia y necesidad sería posible el acceso a dicha información en el ejercicio de sus funciones legítimas de prevención e investigación del delito, descubrimiento de los delincuentes y recogida de los instrumentos, efectos y pruebas del mismo.

No obstante, como se verá en los apartados correspondientes a la conservación y cesión de los datos de tráfico, en esta materia tuvo una gran incidencia la Ley 25/2007, de 18 de octubre, sobre conservación de datos de las comunicaciones electrónicas, que obliga a los operadores que presten tales servicios a conservar determinados datos (entre ellos datos de abonados) generados y tratados en el marco de la prestación de ese servicio y concretamente los previstos en el artículo 3 de dicha ley, necesarios para:

1. Rastrear e identificar el origen de una comunicación.
2. Identificar el destino de una comunicación.
3. Determinar la fecha, hora y duración de una comunicación.
4. Identificar el tipo de comunicación.
5. Identificar el equipo de comunicación de los usuarios o lo que se considera ser el equipo de comunicación.

En relación con los datos referidos a abonados que se recogen en el citado artículo 3, la Ley 25/2007, en su artículo 1 fija un régimen especial a cuyo tenor estos solo pueden ser entregados por los operadores a requerimiento de la autoridad judicial.

Si el acceso a los datos de tráfico conservados por una operadora de comunicaciones al amparo de lo dispuesto en la ley 25/2007 precisa autorización judicial. La reclamación a las operadoras de la identificación del titular a partir de los datos de un dispositivo, o determinar los dispositivos de los que es titular una persona concreta, realizada por la Policía Judicial o el Ministerio Fiscal en el curso de una investigación concreta no lo precisa; tal y como establece el art. 588 ter m. En este caso, observamos que el razonamiento es que se respeta el principio de proporcionalidad de la medida, ya que el derecho a la intimidad del interesado se

vería muy débilmente afectado y primaría el interés público en la investigación y esclarecimiento de un hecho delictivo.

5.8.4. Acceso a datos que no forman parte de un proceso de comunicación

Se presenta mucho más complejo el caso acerca de si el Fiscal y la policía pueden acordar el acceso a documentos no integrados en un proceso de comunicación y archivados en teléfonos móviles, ordenadores o asimilados, cuando concurran razones de urgencia.

Como ya se ha señalado, excepcionalmente se ha legitimado a la Policía para que con la suficiente y precisa habilitación legal realice determinadas prácticas que constituyen una injerencia leve en la intimidad de las personas, siempre que se hayan respetado las exigencias dimanantes del principio de proporcionalidad[390].

La apertura de una agenda y la lectura de lo encontrado en ella incide claramente en el derecho a la intimidad, pero no en el secreto de las comunicaciones. Igualmente, se había puesto de manifiesto que, a pesar de las múltiples funciones de un ordenador personal, el acceso a su contenido podrá afectar bien al derecho a la intimidad personal, bien al derecho al secreto de las comunicaciones en función de si lo que resulta desvelado a terceros son, respectivamente, datos personales o datos relativos a la comunicación[391].

En España, la STC 115/2013, de 9 de mayo afirmó claramente entre el acceso a la agenda de un móvil, que no precisa autorización judicial, y el acceso al listado de llamadas, que sí lo precisaría. En este sentido, cuando el acceso de la Policía al teléfono móvil del investigado se limita a los datos recogidos en el archivo de contactos telefónicos pero no al registro de llamadas efectuadas y/o recibidas, debía concluirse que dichos datos no forman parte de una comunicación actual o consumada, ni proporcionan información sobre actos concretos de comunicación

[390] STC 142/2012, de 2 de julio y STC 281/2006, de 9 de octubre
[391] STC 142/2012, de 2 de julio; 173/2011, de 7 de noviembre y STS 663/2011, de 7 de julio

pretéritos o futuros. Con el acceso a la agenda de contactos telefónicos no se obtiene información concerniente a la transmisión de comunicación emitida o recibida por el celular, sino únicamente un listado de números telefónicos introducidos voluntariamente por el usuario del terminal sobre los que no consta si han llegados a ser marcados.

En una ponencia presentada en el curso de Formación de Fiscales "Uso de las nuevas tecnologías y nuevas formas de delincuencia" que se celebró en el Centro de Estudios Jurídicos los días 27 al 28 de octubre de 2016, Vazquez Seco afirmó que "*Habrá que esperar que la jurisprudencia clarifique ciertos supuestos controvertidos, como son los datos de posicionamiento que emiten por ejemplo los terminales móviles al margen de una comunicación concreta, como un teléfono móvil encendido, aunque no se utilice para ninguna comunicación, al desplazarse el usuario el terminal va saltando de una celda a otra en busca de señal según la antena de comunicación más próxima con la que se conecte, y esa información puede ser recuperada, y la cuestión está en que esos datos de localización se generan al margen de una comunicación concreta; parece claro que esa información permite seguir los movimientos de su titular, por lo que afecta al derecho a la intimidad y por tanto de la cobertura de una autorización judicial; o supuestos que sin duda se generaran en el futuro con la expansión de la denominada "internet de las cosas" donde la comunicación no es entre personas sino entre máquinas, aunque utilizando el mismo razonamiento esos aparatos electrónicos se comunican previa programación de una persona, y esa programación junto a las comunicaciones realizadas en ejecución de la misma parece claro que también están bajo el ámbito reservado protegido por el derecho a la intimidad*"[392].

Una primera doctrina consideraba que lo decisivo para la delimitación del contenido de los derechos fundamentales recogidos en los arts. 18.1 y 18.3 CE no era el tipo de soporte, físico o electrónico, en el que la agenda de contactos se

[392] VÁZQUEZ SECO, L. (2017). «Incorporación de datos al proceso. Vigencia de la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a redes públicas e interpretación de la ley a la luz de la reforma operada por la LO 13/2015». Madrid: Centro de Estudios Jurídicos. Universidad Complutense de Madrid, págs. 19-24

encontrara ni el hecho de que la agenda fuese una aplicación de un terminal telefónico móvil, sino el carácter de la información a la que se accede[393].

España ha superado de alguna forma con esta discusión, a partir de la sanción de su Ley de Enjuiciamiento Criminal, con la aplicación del artículo 588 sexies c apartados 3º y 4º, que permite a la policía, en caso de urgencia, acceder al contenido de los dispositivos sea cual sea el mismo, sin especificar si se accede a datos vinculados o no a procesos de comunicación y siempre que se informe al juez competente dentro del plazo máximo de veinticuatro horas. Pero esta posibilidad de que acceda la policía a una agenda de teléfono móvil, sin autorización judicial, se limita exclusivamente a los supuestos de urgencia, que se detallarán más adelante.

5.8.5. Interceptación de conversaciones en el espacio público.

Existen medios en internet, como los chats o foros, que permiten comunicarse a varias personas simultánea y públicamente en tiempo real. Obviamente, cuando las comunicaciones son accesibles para cualquier usuario de internet, no pueden tener la consideración de conversaciones privadas, pues es el propio usuario de la red quien se introduce en la misma y asume que muchos de los datos se convierten en públicos para todos los usuarios. Por ello, estas modalidades no pueden considerarse amparadas por el derecho fundamental al secreto de las comunicaciones, por lo que no precisan de autorización judicial para su grabación u observación, en virtud de la máxima de que “no se precisa autorización judicial para conseguir lo que es público”, siempre que nos encontremos en cumplimiento de los principios ya desarrollados en este capítulo por supuesto.

Lo mismo es predicable respecto a la intervención de comunicaciones emitidas por radiofrecuencia, que no necesita autorización judicial al quedar fuera de la reserva que establece el artículo 18.3 de la Constitución Española. En el caso argentino, como hemos visto en la primer parte de esta tesis doctoral, la conducta

[393] STC 142/2012, de 2 de julio

prohibida en el segundo párrafo del art. 183, es la interceptación de comunicaciones que sean de sistema de carácter privado o de acceso restringido.

En consecuencia, si atendemos a la naturaleza de las comunicaciones de radio que, por el medio técnico en el que se desenvuelven siempre son públicas, nunca precisarán de una autorización judicial para hacer público lo que ya lo es. Asimismo, podría interpretarse en relación a las comunicaciones electrónicas que se transmiten a través de una red abierta y pública, donde podría suponerse una tácita renuncia a la expectativa de privacidad de dicha conversación.

En todo este contexto, consideramos necesario hacer un desarrollo sobre una categorización sobre los datos, aceptada a nivel internacional, y que denominaremos -con cierta finalidad pedagógica- como “la regla de los 3 escalones”[394].

5.8.6. La regla de los 3 escalones

A través de la misma, se pretende aclarar las distintas categorías de información a la cuál es posible acceder en el contexto de una investigación penal, y sobre todo, que nivel de afectación a los derechos implica cada una de ellas.

Sin embargo, como en toda buena construcción, nuestra escalera no podrá estar flotando en el aire sino deberá estar apoyada sobre una base firme, sobre algún piso que -en nuestra elaboración teórica- serán aquellos datos para en cuyo acceso no se considere que existe una afectación indebida a los derechos.

Esta primera base estará apuntalada sobre un criterio -en principio ampliamente aceptado por la jurisprudencia- que interpreta como válida la incorporación como elemento de prueba, en el marco de una investigación penal, de aquellos datos que sean considerados como públicos, es decir, cuyo acceso sea posible de forma irrestricta y sin vulnerar ninguna barrera técnica o jurídica.

[394] TEMPERINI, Marcelo; Delitos informáticos y cibercrimen; Técnicas y tendencias de investigación penal y su afectación a los derechos constitucionales; Cibercrimen II. Nuevas conductas penales y contravencionales. Inteligencia artificial aplicada al Derecho penal y procesal penal. Novedosos medios probatorios para recolectar evidencia digital. Cooperación internacional y victimología. Directora y Coordinadoras: Dupuy, Daniela - Kiefer, Mariana y otros. Año 2018. Edición 1ª

Un claro ejemplo de esta primera categoría de información, será aquella que es posible obtener a través de la utilización de las difundidas técnicas de OSINT (Open Source Intelligence) las cuáles precisamente apuntan a la búsqueda, identificación y procesamiento de información sobre fuentes abiertas, es decir, sobre aquellas que pueden obtenerse de forma pública y por lo tanto -en principio- no existe afectación alguna sobre la privacidad del titular de esos datos.

Dentro de la jurisprudencia, un caso en Argentina[395] logró condenar a una persona por homicidio agravado gracias a que a través de una identificación por su perfil de Facebook, se logró identificar al criminal. Se trató de un caso de homicidio sobre un hombre que fue asesinado mientras dormía en la vía pública por dos personas que lo rociaron con combustible y luego lo prendieron fuego. Los vecinos del lugar señalaron que uno de los autores se apodaba "Chucky". Gracias a la mención de ese nombre, los investigadores del caso lograron dar con el principal sospechoso, Alexis Bejarano, quien tenía un perfil público en Facebook. Se hizo una rueda de reconocimiento y una de las testigos no dudó de que se trató de uno de los autores.

Ante dicha situación la defensa del condenado interpuso una queja que sostenía que había que equiparar a la prueba informática por la que se obtuvo el perfil de Facebook del encartado, con la correspondencia epistolar. La defensa aseguró que debía existir orden judicial para obtener la información del correo electrónico y las redes sociales.

Sin embargo, el Tribunal sostuvo que la red social "Facebook" es un sitio web que se encuentra disponible para cualquier usuario de la red y se utiliza para que sus usuarios puedan intercambiar comunicación fluida y compartir contenido de forma sencilla a través de Internet. A partir de sus características públicas la página de Facebook propiedad del imputado "*no goza de la protección de la privacidad como la clásica vía postal*". Según la Casación Federal, si bien para el funcionamiento y utilización de la red social "*se requiere indispensablemente de un prestador del servicio, el nombre de usuario y clave de acceso destinados a impedir*

[395] Fallo "Bejarano, Alexis s/Recurso de Casación" - Sala IV de la Cámara Federal de Casación Penal, Argentina

que terceros extraños se entrometa en los datos y contenidos que se emiten y reciben", en el caso el perfil del condenado "*era público y casi toda la información que compartía podía ser vista por cualquier persona que accediera a través de internet a la página". "La página de Facebook no puede ser considerada la 'correspondencia epistolar' que protege la Constitución Nacional, razón por la cual el modo en que fue obtenida e incluso su incorporación como prueba al juicio, mal puede violar la garantía contenida en el art. 18 de la CN*", señalaron los camaristas.

Hacia el final de la sentencia se afirma que "*a partir de lo expuesto, entiendo que el procedimiento por el cual se obtuvo e incorporó como prueba la página de Facebook mediante la cual se pudo corroborar que el sujeto apodado "Chucky" se correspondía con el nombre y fotografía que figuraban en ese perfil de la red social fue realizado conforme a las disposiciones legales vigentes sin afectar la garantía que prohíbe intromisiones arbitrarias en la intimidad y privacidad del imputado y por ello propongo rechazar el presente agravio*".

Es decir, queda claro en base a este último párrafo el criterio adoptado, donde se entiende que las garantías constitucionales que prohíben la intromisión arbitraria en la intimidad y privacidad del imputado, no se encuentran afectadas cuando se trata de información disponible de forma pública e irrestricta.

A modo de comentario final, aclaramos que distinto hubiese sido el análisis jurídico si se hubiese tratado de una imagen publicada con alguna limitación sobre la privacidad (amigos o amigos de mis amigos).

5.8.6.1. El primer escalón: los datos de abonado

Superada la explicación sobre la base de los datos públicos, es momento de avanzar hacia nuestro primer escalón: los datos de identificación de usuario, o también denominados "datos de abonado" o en el caso de redes sociales, más conocidos como BSI (Basic Subscriber Information).

En este primer escalón encontraremos distintos tipos de información identificatoria relacionada al titular de la cuenta o del servicio consultado. A nivel internacional contamos con una definición en el Convenio de Cibercrimen de

Budapest[396]. En el artículo 18 donde se regula la "orden de presentación", en su inc. 3, se define:

> *"A los efectos del presente artículo, por «datos relativos a los abonados» se entenderá toda información, en forma de datos informáticos o de cualquier otra forma, que posea un proveedor de servicios y esté relacionada con los abonados a dichos servicios, excluidos los datos sobre el tráfico o sobre el contenido, y que permita determinar:*
>
> *a) El tipo de servicio de comunicaciones utilizado, las disposiciones técnicas adoptadas al respecto y el periodo de servicio;*
>
> *b) la identidad, la dirección postal o geográfica y el número de teléfono del abonado, así como cualquier otro número de acceso o información sobre facturación y pago que se encuentre disponible sobre la base de un contrato o de un acuerdo de prestación de servicios;*
>
> *c) cualquier otra información relativa al lugar en que se encuentren los equipos de comunicaciones, disponible sobre la base de un contrato o de un acuerdo de servicios".*

En la base de la definición, existe una conceptualización casi por exclusión, al decir que es toda información (generalmente datos personales) que posea un proveedor de servicios, relacionada con el abonado del servicio, que no sean ni datos de tráfico ni datos de contenido. Por otro lado, en una guía publicada entre la documentación oficial de Naciones Unidas[397] se detallan algunos de los datos de suscriptor que podrán estar disponibles para la consulta judicial:

- Nombre de la cuenta, nombre de usuario o de acceso
- Nombre y Apellido registrados
- Domicilios registrados
- Correo electrónico registrados

[396] Convenio de Ciberdelincuencia del Consejo de Europa de Budapest, de 23 de noviembre de 2001
[397] Guide to Obtaining Communication Service Provider Evidence from the United States, United Nations, Url: http://www.un.org/en/sc/ctc/docs/2015/CSP%20Guidance%202015.pdf

- Números de teléfonos asociados a la cuenta
- Dirección IP utilizada al momento de la creación de la cuenta
- Fecha y hora de creación de la cuenta
- Información de sesiones iniciadas (user agent, IP de acceso, fecha y duración)
- Otros datos identificatorios del suscriptor (formas de pago, tipos y números de tarjetas de crédito utilizadas, etc.)

Vale destacar que los datos identificatorios disponibles dependen del tipo de servicio que estemos analizando, toda vez que dentro de la categoría genérica de los CSP[398], podemos incluir tanto los ISP[399] como toda otra plataforma de prestación de servicio de comunicaciones, como redes sociales, sitios de comercio electrónico, hosting, etc.

A modo de ejemplo, en el caso de tratarse de un ISP estaremos hablando de los datos personales del titular de la línea o servicio, tales como nombre, apellido, domicilio, tipo de servicio contratado, número de usuario, formas de pago utilizadas, tarjetas de crédito utilizadas, entre otros datos. En el caso de otros servicios, como redes sociales, podrá considerar también que se considera parte de estos datos básicos del suscriptor, algunos datos tales como el correo electrónico, dirección IP desde la cuál se ha generado la cuenta, incluso las direcciones IP de los últimos accesos a la misma, pueden formar parte de este paquete de datos (BSI).

Este primer escalón, como categoría inicial de datos que avanzan sobre un ámbito de privacidad, presentan como característica que nos encontramos ante la presencia de datos identificatorios que gozan de la protección de los datos de carácter personal, por lo que les serán aplicables todas aquellas normativas relacionadas a la protección de datos personales, bajo la inteligencia que se trata de información que permitiría identificar o hacer identificable a una persona[400].

[398] CSP: Communication Service Provider (Proveedor de Servicios de Comunicación)
[399] ISP: Internet Service Provider (Proveedor de Servicio de Internet)
[400] Art. 2 de la Ley Nº 25.326 de Protección de Datos Personales en Argentina.

Una de las primeras discusiones clásicas que podría darse dentro de esta categoría, tenía relación con la naturaleza de la dirección IP, acerca de si ésta podía o no ser considerada como un dato de carácter personal y en consecuencia, debía aplicarse todo el andamiaje protectorio correspondiente. En este sentido el Informe 327/2003[401] de la Agencia de Protección de Datos Española (AGPD) ha señalado que "aunque no siempre sea posible para todos los agentes de Internet identificar a un usuario a partir de datos tratados en la Red, desde esta Agencia de Protección de Datos se parte de la idea de que la posibilidad de identificar a un usuario de Internet existe en muchos casos y, por lo tanto, las direcciones IP tanto fijas como dinámicas, con independencia del tipo de acceso, se consideran datos de carácter personal resultando de aplicación la normativa sobre protección de datos."

En la parte final, el mismo informe nos deja una sencilla reflexión sobre la interpretación de los datos personales, que es plenamente aplicables a los demás datos identificatorios desarrollados en esta categoría. Sostiene la AGPD que "En cuanto a la consideración de los "log-in" de acceso a Internet o a páginas personales como datos de carácter personal, resultarán de aplicación las consideraciones que se realizan en párrafos anteriores. Si identifica de forma directa al usuario, no hay duda de que estaremos ante un dato de carácter personal, por el contrario si este es anónimo, en principio no sería un dato de carácter personal, pero si, por ejemplo, el proveedor de servicios de Internet a través de ese "log in", puede identificar al usuario con el que tiene un contrato de acceso a Internet, sí será considerado como un dato de carácter personal.".

Superado este primer desafío, y quedando claro que estamos ante la presencia de un conjunto de datos personales que hacen a la identificación de una persona, un segundo interrogante sale a la luz en relación a los requisitos legales que deberán cumplirse para poder solicitar este tipo de datos: ¿Es necesaria una autorización judicial para acceder a esta información? ¿O será suficiente un pedido realizado por el Fiscal en el marco de las potestades establecidas para dirigir una investigación penal?.

[401] AGPD: Agencia de Protección de Datos Española, Carácter de dato personal de la dirección IP. Informe 327/2003, Url: https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/otras_cuestiones/common/pdfs/2003-0327_Car-aa-cter-de-dato-personal-de-la-direcci-oo-n-IP.pdf

Sobre este interrogante se ha planteado un interesante caso en Argentina[402], en el cuál en el marco de la investigación de un caso de distribución de pornografía infantil, el allanamiento sobre el domicilio del imputado había sido posible gracias a los datos de identificación suministrados por dos CSP (Telecom y Microsoft), pedido de información que había sido solicitado solamente por el Fiscal que llevó adelante la causa, es decir, sin autorización judicial.

En este caso, los jueces de Cámara para declarar la nulidad del requerimiento de juicio argumentaron "*que las direcciones IP (Internet Protocols) son datos de carácter personal protegidos por la ley n° 25.326 y que, por esa razón, la solicitud de aquellos informes debía equipararse a una "interceptación telefónica" y debió solicitarse la pertinente orden judicial, de conformidad con lo establecido en el art. art. 93, in fine, del CPPCABA*". En ese sentido, afirmaron que "*una amplia protección al derecho a la intimidad obliga a entender que los datos personales de quien afirmó ser usuario de un correo electrónico asociado a un protocolo de internet (al crear la cuenta de correo electrónico), registrados por las firmas de telecomunicaciones se encuentran alcanzados por la regla que ampara la privacidad y sólo con orden judicial pueden requerirse informes sobre estos datos, en principio, reservados*".

Siguiendo con el voto del Juez José Casás, afirma "*Sin embargo, lejos de formular argumentación alguna que permita sostener dicha afirmación, los magistrados omitieron explicar por qué razón correspondería equiparar, a la luz de la expectativa de intimidad del individuo, los datos de contenido y los datos de tráfico de una comunicación, con la simple identificación de un usuario. Dicha circunstancia resultaba de vital trascendencia a los fines de analizar la problemática constitucional planteada en el caso concreto. En tercer lugar, tampoco la invocación de la ley de protección de datos personales (ley n° 25.326) resulta dirimente para la solución del caso porque no está en discusión que la información requerida a las empresas mencionadas en las resultas perseguía la obtención de "datos personales". Lo que no advierten los camaristas es que la propia ley prevé que dicha información puede ser recabada, sin que se requiera el consentimiento del titular, en el ejercicio de funciones propias de los poderes del Estado (art. 5.2.b) y también cuando esos*

[402] Fallo "Ministerio Público —Fiscalía de Cámara Norte de la CABA— s/ queja por recurso de inconstitucionalidad denegado en 'A, C s/ infr. art. 128.2, párr. 2°, CP'"

datos se limitan al nombre, documento y domicilio de la persona en cuestión (art. 5.2.c). No otra cosa se pretendió respecto del titular de la IP aportada a la investigación cuando el fiscal, en el ejercicio de sus funciones de instructor, formuló el cuestionado pedido de informes".

En este primer voto, se analiza con extrema precisión la confusión que ha dado lugar al planteo, y es la confusión entre los datos identificatorios, datos de tráfico y datos de contenido, toda vez que erróneamente (a nuestro criterio) la Cámara interpretó que los datos identificatorios son "datos de contenido", exigiendo en consecuencia el requisito de autorización judicial para su obtención.

En un segundo voto, el Dr. Luis Lozano, se analiza aún con mayor precisión el aspecto procesal que aquí nos interesa, sobre los alcances en las medidas de investigación que puede llevar adelante un fiscal: "*asiste razón al MPF en cuanto manifiesta que ese pronunciamiento ha extendido el alcance de la norma local sobre cuya base aquel se sostiene a un supuesto no contemplado e importa una declaración implícita de inconstitucionalidad de las facultades de investigación que la ley le confiere. Este artículo (art. 93 del CPPCABA[403]) inviste al fiscal de un cúmulo de facultades para reunir prueba. Lo hace en términos en que incluye no sólo las expresamente contempladas sino también "…todas las medidas que considere necesarias para el ejercicio de sus funciones". Reserva algunas al juez, rodeándolas así de una garantía específica sólo posible en el sistema acusatorio, ya que, en ese sistema, el órgano que decide, el juez, a diferencia del juez inquisidor, cuya jurisdicción suma o absorbe atribuciones propias de la acción fiscal, no tiene fijada la meta de investigar —en efecto, en los procesos de tipo acusatorio, el juzgador, árbitro de una contienda entre partes legitimadas, carece de iniciativa propia en la investigación y de poderes autónomos para investigar la verdad de los acontecimientos—, sino que está colocado en situación de ponderar imparcialmente*

[403] Ley Nº 2303/07, Código Procesal Penal de la Ciudad Autónoma de Buenos Aires: Art. 93: "A fin de desarrollar la investigación preparatoria el/la Fiscal podrá citar a testigos, requerir los informes y peritajes que estime pertinentes y útiles, practicar las inspecciones de lugares y cosas, disponer o requerir secuestro de elementos y todas las medidas que considere necesarias para el ejercicio de sus funciones. Deberá solicitar orden judicial para practicar allanamientos, requisas o interceptaciones de comunicaciones o correspondencia" Url: http://www.buenosaires.gob.ar/areas/leg_tecnica/sin/norma_pop.php?id=98678&qu=c&rl=0&rf=0&im=0&menu_id=21544

entre el interés del pueblo en conocer y probar y el del sujeto de preservar su privacidad."

Este interesante análisis establece con claridad las potestades investigativas del fiscal, en el marco de un sistema acusatorio, donde la norma procesal penal establece expresa reserva para determinadas medidas, que el legislador ha considerado que afectan en mayor medidas las garantías constitucionales (allanamientos, requisas o interceptación de comunicaciones o correspondencia).

A modo de conclusión de este primer escalón, y de respuesta sobre los interrogantes planteados, destacamos que los datos identificatorios (o de abonado como se denominan en España) son datos de carácter personal, que avanzan sobre una primera barrera de privacidad de la persona investigada, pero que no deben confundirse con los datos de tráfico, ni menos aún, con los datos de contenido.

Desde un punto de vista jurídico, podemos interpretar que esos datos personales -de acuerdo a la normativa aplicable- podrán ser accedidos sin contar con el consentimiento de su titular para aquellos casos de ejercicios de funciones propias del Estado (art. 5.2.b de la Ley Nº 25.326 de Argentina), por lo que en el contexto de una investigación penal -en el marco de un proceso acusatorio- se considera suficiente para su acceso una orden librada por el fiscal a cargo, no siendo necesario contar con una autorización judicial, reservada para otras instancias de mayor afectación de los derechos.

5.8.6.2. El segundo escalón: los datos de tráfico

En este segundo escalón encontraremos una categoría distinta de datos, conocidas como datos de tráfico, datos asociados, datos transaccionales, metadatos de la comunicación, entre otras denominaciones que podrán encontrarse en la doctrina y jurisprudencia.

Nuevamente consultando el Convenio de Cibercrimen de Budapest, donde si bien su artículo 1 contiene muy pocas definiciones, entre ellas encontramos la de "datos de tráfico", que de acuerdo a este instrumento son "*...cualquier dato informático relativo a la comunicación por medio de sistema informático, generado*

por el sistema informático que forma parte de la cadena de comunicación, indicando origen, destino, ruta, hora, fecha, tamaño, duración o tipo de servicio subyacente".

De acuerdo a esta definición, podríamos interpretar que los registros de un servidor que guarda las comunicaciones electrónicas entrantes y salientes, es un listado de datos de tráfico, toda vez que incluye la dirección IP de origen, dirección IP destino, fecha, hora y ruta de esa comunicación. De la misma forma, esta misma definición es aplicable para las conocidas "listas sábanas" de las llamadas telefónicas, donde es posible identificar el número de línea que realiza la llamada, número de destino, fecha, hora y duración de la comunicación. Es decir, independientemente del detalle que pueda establecerse en relación al tipo de comunicación, lo importante es tener en claro que entre los datos de tráfico nunca podremos encontrar algún tipo de contenido de la comunicación.

En la normativa española podemos encontrar otro concepto similar dentro de la Ley Orgánica de Enjuiciamiento Criminal 13/2015, en el capítulo V sobre "La interceptación de las comunicaciones telefónicas y telemática", en el artículo 588 ter b), define "datos electrónicos de tráfico o asociados" como "*todos aquellos que se generan como consecuencia de la conducción de la comunicación a través de una red de comunicaciones electrónicas, de su puesta a disposición del usuario, así como de la prestación de un servicio de la sociedad de la información o comunicación telemática de naturaleza análoga*"

Teniendo en claro el alcance de su concepto, podremos avanzar hacia quizás una de los tópicos clave de este artículo, que es el argumento jurídico sobre la legitimidad en el acceso a esta clase de información. Discusión que desde ya adelantamos, con el paso de los años se han observado distintas posturas, que intentaremos ir desandando. Entre todas las preguntas que el lector podría realizarse sobre esta temática, elegimos algunas para abordar aquí:

¿Qué nivel de afectación a las garantías constitucionales existe al acceder a los datos de tráfico de una comunicación?

¿Es necesario contar con autorización judicial para poder acceder a un listado de datos de tráfico de las comunicaciones realizadas por una persona?

¿Es constitucional obligar a un proveedor de comunicaciones que realice la guarda de todos los datos de tráfico de las comunicaciones de sus abonados?

Si bien algo ya se ha adelantado en el desarrollo del primer escalón, veremos aquí con mayor profundidad el alcance y protección jurídica de esta segunda categoría de datos. En relación a la primera pregunta, sobre el nivel de afectación de las garantías a través de los datos de tráfico, ya hemos citado uno de los antecedentes más importantes como es el caso Malone anteriormente citado, en el cuál se debatió el alcance en el amparo al secreto de las comunicaciones.

En este denominado leading case, analizado en un reciente y completo estudio del Dr. David Calvo Lopez[404], se reconoció expresamente la posibilidad de que el artículo 8 CEDH[405] pudiera resultar violado por el empleo de un artificio técnico que permita registrar cuáles hayan sido los números telefónicos marcados sobre un determinado aparato, aunque no acceda al contenido de la comunicación misma. Es decir, relacionado a la primera pregunta que nos hemos realizado, podemos responder que en principio existe aceptación jurisprudencial en entender que la protección jurídica de los datos de tráfico, por la potencialidad en la afectación de las garantías que poseen esta categoría de datos, se encuentra asimilada al mismo nivel de protección jurídica que los datos de contenido.

Decimos en principio, toda vez que válidamente el lector podría preguntarse si todos los datos de tráfico afectarían de la misma forma a los derechos constitucionales aquí involucrados. En este sentido, la Circular 1/2013[406] de la Fiscalía General del Estado Español, explica que “no todos los datos digitalizados

---

[404] CALVO LOPEZ, David, “Capacidades de actuación del Ministerio Público Fiscal y la Policía Judicial tras la reforma procesal operada por la Ley Orgánica 13/2015”, Jornadas de Especialistas celebradas en el Centro de Estudios Jurídicos de Madrid, 16 y 17 de Febrero de 2017.

[405] Convenio para la Protección de los Derechos Humanos y de las libertades fundamentales - Art. 8: Derecho al respeto a la vida privada y familiar. 1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia. 2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás.

[406] Fiscalía General del Estado (España) - Circular 1/2013, sobre pautas en relación con la diligencia de intervención de las comunicaciones telefónicas. Url: https://www.fiscal.es/memorias/memoria2014/FISCALIA_SITE/recursos/cir_inst_cons/circular_1_2013.pdf

merecen la consideración de datos propios del contenido material del derecho a la inviolabilidad de las comunicaciones. Debe analizarse la funcionalidad de cada dato para ubicarlo bajo el manto protector del derecho a la intimidad (art. 18.1 CE), del derecho a la inviolabilidad de las comunicaciones (art. 18.3 CE) o del derecho a la protección de datos (art. 18.4 CE), cada uno con su propio sustrato axiológico y, correlativamente, cada uno con una protección de intensidad variable".

Sí que estarían incluidos, como señala la citada Circular, aquellos "datos accesorios pero íntimamente ligados a la propia comunicación" por revelar el origen y destino de la misma, su momento y duración y, por último, los referentes al volumen de la información transmitida y el tipo de comunicación entablada. Son, en definitiva, datos que se generan mientras la comunicación se encuentra en curso.

En similar criterio se ha expresado el Tribunal Supremo en la Sentencia STS 247/2010[407], relacionado a un caso de posesión de pornografía infantil, donde se discutía la validez o no de las medidas de investigación realizadas, y la posible afectación de los derechos constitucionales del imputado. En la sentencia, se realiza una distinción fundamental para resolver cualquier cuestión relativa a los derechos amparados por el artículo 18 CE. En la misma afirma: "*Distinguimos pues dos conceptos: a) Datos personales externos o de tráfico que hacen referencia a una comunicación concreta y contribuyen a desvelar todo o parte del secreto que protege el art. 18-3 C.E EDL 1978/3879; b) Datos o circunstancias personales referentes a la intimidad de una persona (art. 18-1o C.E. EDL 1978/3879), pero autónomos o desconectados de cualquier comunicación, que caerán dentro del derecho a la protección de datos informáticos o habeas data del art. 18-4 C.E. EDL 1978/3879 que no pueden comprometer un proceso de comunicación. Desde esta perspectiva dicotómica la absoluta equiparación de todo tipo de datos de tráfico o externos o la inclusión de todos ellos dentro del derecho al secreto de las comunicaciones comportaría un auténtico desenfoque del problema, pues incorporaría en el ámbito de la protección constitucional del art. 18-3, circunstancias cuyo tratamiento jurídico no debería separarse del que se dispensa a la protección de datos o al derecho a la*

[407] Sentencia nº 247/2010 de TS, Sala 2ª, de lo Penal, 18 de Marzo de 2010, Url fallo completo: https://supremo.vlex.es/vid/-215145099

autodeterminación informática del art. 18-4 C.E. EDL 1978/3879 (véase por todas S.T.S. núm. 249 de 20-5-2008 EDJ 2008/90719)".

En el caso concreto se resolvió que "*es patente que los datos cuyo obtención se pretende por el Fiscal no tienen relación ni afectan ni interceptan ni descubren ni tratan de descubrir una comunicación concreta, sino que por ser preciso para la acción investigadora el conocimiento del domicilio, número de teléfono o identidad del titular del terminal informático que opera en la Red (I.P.), la solicita a la operadora, al objeto de pedir del juez un mandameinto de entrada y registro con fines indagatorios o de investigación de un posible delito, acerca del que se conocen datos indiciarios*".

Esta jurisprudencia, de similar interpretación a la citada anteriormente en Argentina[408] concluye que al no tratarse de datos de tráfico -toda vez que solamente se han solicitado datos identificatorios personales-, no será necesaria la orden judicial para el caso de solicitud de los datos de abonado (nuestro primer escalón), por considerarse que no existe allí una afectación a una comunicación concreta, y por lo tanto, no hay afectación a un derecho constitucional.

Es decir -y ya aquí comenzando con la respuesta a la segunda pregunta planteada-, que sólo ante el análisis positivo sobre si los datos de tráfico solicitados (como suele sucede con el listado de llamadas, o los datos de tráfico de un ISP) permitan afectar la inviolabilidad de las comunicaciones y por lo tanto, la afectación del secreto de las comunicaciones, será necesario contar con autorización judicial de juez competente para poder válidamente acceder a esta segundo escalón o categoría de datos.

A nivel normativo, esta discusión se encontró resuelta dentro de la Ley Orgánica de Enjuiciamiento Criminal 13/2015, en cuyo artículo 588 ter b) exige que la resolución judicial habilitante precise el contenido de la intervención de las comunicaciones telemáticas, que puede venir referido a tres conceptos distintos: a) el mensaje comunicado; b) los datos electrónicos de tráfico o asociados al proceso

[408] Fallo "Ministerio Público —Fiscalía de Cámara Norte de la CABA— s/ queja por recurso de inconstitucionalidad denegado en 'A, C s/ infr. art. 128.2, párr. 2°, CP'"

de comunicación y c) aquellos producidos con independencia del establecimiento o no de una concreta comunicación:

"La intervención judicialmente acordada podrá autorizar el acceso al contenido de las comunicaciones y a los datos electrónicos de tráfico o asociados al proceso de comunicación, así como a los que se produzcan con independencia del establecimiento o no de una concreta comunicación, en los que participe el sujeto investigado, ya sea como emisor o como receptor, y podrá afectar a los terminales o los medios de comunicación de los que el investigado sea titular o usuario".

Por último, en relación a un adelanto de respuesta de la tercera pregunta sobre la constitucionalidad de la obligación de guarda de esta categoría de datos, informamos al lector que si bien no ahondaremos en todos los argumentos jurídicos que deberían tratarse para hacer un desarrollo adecuado y serio del tema, que por cuestiones de tiempo y espacio que exceden la labor del presente trabajo, citaremos solamente algunos aspectos centrales y medulares de dicha discusión.

En el año 2006 la Unión Europea aprobó la Directiva sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones, popularmente conocida como "Directiva de retención de datos"[409], que a lo largo de los años fue gestando normativas internas de los distintos países europeos que regulando sus propias condiciones para la conservación de este tipo de datos.

El objetivo buscado por la normativa general era obligar a los proveedores de servicios de comunicaciones electrónicas de acceso público o red pública de comunicación a conservar los datos generados o tratados por los mismos, para garantizar que los datos estén disponibles con fines de investigación, detección y enjuiciamiento de delitos graves, donde cada país determinada su interpretación de lo que se consideraban delitos graves de acuerdo a su propia normativa penal.

[409] DIRECTIVA 2006/24/CE, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE. Url: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:ES:PDF

En la práctica, la aplicación de la Directiva implicaba que existía una retención de datos de tráfico de todos los usuarios, por un tiempo determinado (entre 6 meses y 2 años por lo general) independientemente si los mismos estaban o no siendo parte de una investigación penal que justificaba el acceso a dichos datos, y por lo tanto, la afectación de sus garantías constitucionales.

Sin embargo, esta Directiva no fue siempre aceptada por todos, y ya en su momento había generado una gran polémica y controversia, ya que para algunos sectores su articulado implacable una vulneración a la privacidad de los ciudadanos. De hecho, en algunos países nunca fue tenida en consideración para su regulación interna, ya que se entendía que su regulación era inconstitucional. Ya en el 2010, el Tribunal Constitucional alemán[410] advirtió (como ya venía haciendo con otros casos anteriores[411]) el riesgo de que el uso de la tecnología, a través del acopio y cruce masivo de datos, pueda dar lugar a la creación de los referidos "perfiles de personalidad" de los ciudadanos hasta el punto de llegar a influir de manera determinante en el comportamiento de los individuos, lo cual entiende que no sólo va en detrimento de las posibilidades de desarrollo individual de los individuos, sino también de la comunidad, porque la autodeterminación es una condición funcional elemental de una nación democrática libre, fundada en la capacidad de sus ciudadanos para cooperar y actuar.

Con motivo de un recurso de inconstitucionalidad contra las reformas que tenían por misión incorporar al Ordenamiento jurídico germano la Directiva Europea de retención de datos, el Tribunal Constitucional alemán declaró en su Sentencia de 2 de marzo de 2010[412] que dicha regulación vulneraba dos principios clave: el principio de proporcionalidad (*Verhältnismäßigkeit*) y el principio de determinación jurídica o claridad legal (*Normenklarheit*), pues aunque la efectividad de la persecución criminal, la defensa de la Seguridad y el cumplimiento de las tareas de los servicios de inteligencia son fines legítimos que pueden constituir una injerencia justificada en el secreto de las telecomunicaciones, y aunque tal Derecho

[410] Alemania prohíbe la retención de datos telefónicos y de internet, Url: https://www.libertaddigital.com/internet/alemania-prohibe-la-retencion-de-datos-telefonicos-y-de-internet-1276386134/
[411] BverfG, 1 BvR 370/07, de 27 de febrero de 2008
[412] BVerfG, 1 BvR 256/08, que resuelve los procesos BvR 256/08, 263/08 y 586/08.

Fundamental no prohíbe cualquier almacenamiento de datos de tráfico, la regulación impugnada suponía un almacenamiento desproporcionado "*con una extensión como hasta ahora el Ordenamiento no había conocido previamente, pues abarca todo el período de seis meses y prácticamente todos los datos de tráfico de las comunicaciones de todos los ciudadanos sin conexión con una conducta reprochable atribuible, incluso de modo abstracto, a una peligrosidad o una situación cualificada (…). Dependiendo de la utilización de las telecomunicaciones y el futuro de tal aumento de la densidad de almacenamiento, puede permitir la producción significativa de perfiles de personalidad y de movimiento de prácticamente todos los ciudadanos, aumenta el riesgo de los ciudadanos a estar expuestos a mayores y posteriores investigaciones, sin ni siquiera el motivo para el que se ha dado el uso, y evoca un sentimiento de vaga amenaza que puede afectar a un ejercicio imparcial de los derechos fundamentales en muchos ámbitos*"[413].

Siguiendo esta esta última postura más crítica de la Directiva Europea, citaremos un importante trabajo de análisis realizado por el Fiscal Luis Vázques Seco[414], quien a modo de resumen de su trabajo, expresa: "*ya desde su promulgación, desde instancias tanto privadas como institucionales se alzaron voces poniendo de relieve aspectos de la Directiva 2006/24/CE que debían ser modificados. Con el paso del tiempo se constató que lejos de armonizar y acercar las legislaciones de los Estados miembros sobre la materia provocó todo lo contrario, una diversidad de regulaciones muy discrepantes en aspectos como el principio de proporcionalidad, los niveles de seguridad de los datos, los procedimientos y requisitos para su utilización, etc., que causaron otro efecto no menos importante, cual es que los operadores de telecomunicaciones, según el Estado donde prestaran sus servicios, se veían sometidos a condiciones totalmente dispares que se traducían fundamentalmente en el coste de los servicios ofertados que a su vez repercutían en los consumidores (los costes de conservar los datos 6 meses son muy inferiores a los generados por la conservación durante 2 años). Y lo*

[413] ORTIZ PRADILLO, Juan Carlos, "La investigación del delito en la era digital: Los derechos fundamentales frente a las nuevas medidas tecnológicas de investigación". Estudios de Progreso – Fundación Alternatives, Url: http://www.falternativas.net/public/storage/actividades_descargas/b78e188fdcae153bcd14b71e5ca618e7.pdf

[414] El Dr. Luis Vázquez Seco es Fiscal Delegado de Criminalidad Informática en la Fiscalía Provincial de La Coruña, España.

mismo en cuanto a la eficacia de las investigaciones policiales, ya que había Estados que permitían utilizar dichos datos para esclarecer prácticamente cualquier delito, mientras otros los restringían a sólo unos pocos, por lo que según el Estado donde se encontrarán almacenados los datos, el resultado de la investigación sería muy distinto"[415].

Años más tarde, tras varias declaraciones de inconstitucionalidad a lo largo del viejo continente, finalmente la Sentencia del Tribunal de Justicia de la Unión Europea de 8 de abril de 2014, al resolver las cuestiones prejudiciales planteadas respectivamente por la *High Court of Ireland* (Irlanda) y el *Verfassunsgerichtshof* (Tribunal Constitucional de Austria), terminó anulando la Directiva 2006/24/CE del Parlamento Europeo, en base a que si bien las obligaciones de conservación y puesta a disposición de datos sobre comunicaciones a que se refiere son necesarias para posibilitar su utilización en la prevención, detección y persecución de delitos graves, la considera desproporcionada, ya que pese a suponer una injerencia de gran magnitud en los derechos fundamentales a la privacidad y protección de datos de carácter personal, no regula debidamente las garantías que deben servir de contrapeso a tal injerencia.

A modo de resumen podríamos afirmar que el fundamento jurídico principal por el cuál se empezaron a declarar la inconstitucionalidad de distintas normativas europeas relacionadas a la retención de datos de tráfico, es la falta de proporcionalidad, la falta de un adecuado equilibrio o balance entre la afectación a los derechos fundamentales que dicha retención de datos provoca, frente a la utilidad que dichos datos representan en las investigaciones de delitos (graves), marcada por los insuficientes controles o requisitos que justifiquen tales avances sobre estos derechos.

[415] VAZQUEZ SECO, Luis, "Retención obligatoria de datos de tráfico de las comunicaciones telefónicas y/o electrónicas. análisis de la sentencia del tribunal de justicia de la unión europea de 8 de abril de 2014 en los asuntos acumulados c-293/12 y c594/12 (Digital Rights Ireland y Seitlinger y otros), Url: https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/Ponencia%20del%20Sr%20Vazquez%20Seco.pdf?idFile=7b863478-eba5-4cbe-8160-859f2387e853

5.8.6.3. El tercer escalón: los datos de contenido

Hemos llegado al tercer y último escalón en nuestra construcción jurídica, generalmente conocidos como datos de contenido y que son, desde el punto de vista de la afectación de los derechos, el nivel más alto de intromisión sobre las garantías constitucionales.

Si bien su concepto no se encuentra definido de forma directa en la Convención de Budapest, podremos ensayar uno a través de la comparación con los propios datos de tráfico. Un reciente estudio sobre "Retención y Privacidad de Datos"[416], los compara afirmando que "*al realizar un envío por correspondencia los datos de tráfico o metadatos son el sobre y las direcciones del remitente y destinatario mientras que los datos de contenido son la carta misma*".

Debemos entender entonces por datos de contenido a la comunicación en sí misma, al propio mensaje que un emisor envía a uno o más receptores, independientemente del medio utilizado (carta, fax, llamada telefónica, whatsapp o correo electrónico). Es decir, que ya no son datos relativos a la comunicación en sí, ya no es el continente sino el contenido -concepto jurídicos si los hay-.

Existe consenso a nivel doctrinario que este tipo de información implica el nivel de afectación más profunda que podría pensarse a nivel jurídico, superando todas las barreras sobre la privacidad del titular, accediendo y conociendo sus comunicaciones, donde se supone que el Estado ha considerado como indispensable a los fines de la averiguación de la verdad de los hechos -y que no existe otra vía menos invasiva- la necesidad de acceder y conocer el contenido de esas comunicaciones privadas.

Todos los derechos repasados al comenzar este artículo son afectados en este último nivel: El derecho a la intimidad, la privacidad, el secreto de las comunicaciones, en el fondo, todos derivados del derecho humano a la dignidad. En consecuencia de los niveles de afectación de los derechos que representa, no queda lugar a dudas sobre la necesidad de autorización judicial -debidamente fundada- para poder acceder a los datos de contenido como última categoría de información.

[416] The Social Engineering Unit, "Retención y Privacidad de Datos: Algunas Lecciones Derivadas de las Diversas Prácticas Internacionales", Url: http://the-siu.net/siu_0k/pdf/SIU-RetencionPrivacidad.pdf

En la práctica y en concordancia con lo expuesto en la guía internacional para la obtención de evidencia[417], además de la necesidad de una resolución judicial que ordene al proveedor de servicios de comunicación aportar esta categoría de información, las empresas también solicitan que exista lo que se considera causa probable, que en Estados Unidos es el nivel mismo de exigencia jurídica que se exige para poder -por ejemplo- solicitar una orden de allanamiento a un domicilio.

No debe considerarse a priori que estos requisitos se tratan de un capricho de las empresas privadas -al menos de forma genérica- sino más bien es una exigencia derivada de un mandato constitucional agregado en el cuarta enmienda de los Estados Unidos, en el cuál se afirma:

> *"El derecho de los habitantes de que sus personas, domicilios, papeles y efectos se hallen a salvo de pesquisas y aprehensiones arbitrarias, será inviolable, y no se expedirán al efecto mandamientos que no se apoyen en un motivo verosímil, estén corroborados mediante juramento o protesta y describan con particularidad el lugar que deba ser registrado y las personas o cosas que han de ser detenidas o embargadas."*[418]

Es decir, las órdenes deben mencionar una causa probable, ratificada mediante juramento o declaración, y describir minuciosamente el lugar donde se realizará la pesquisa y los objetos que se secuestrarán.

Podría aquí el lector realizarse una nueva serie de preguntas:

- ¿Puede el Estado intervenir en cualquier tipo de comunicación? ¿o existen casos de comunicaciones -electrónicas o no- que deberían quedar fuera del alcance del Estado?
- ¿Es posible que el Estado afecte las garantías constitucionales en el marco de la investigación penal?

Para dar respuesta a tales interrogantes, avanzaremos en una breve pero muy importante sección dedicada a los principios y límites a tener en cuenta en las medidas de investigación.

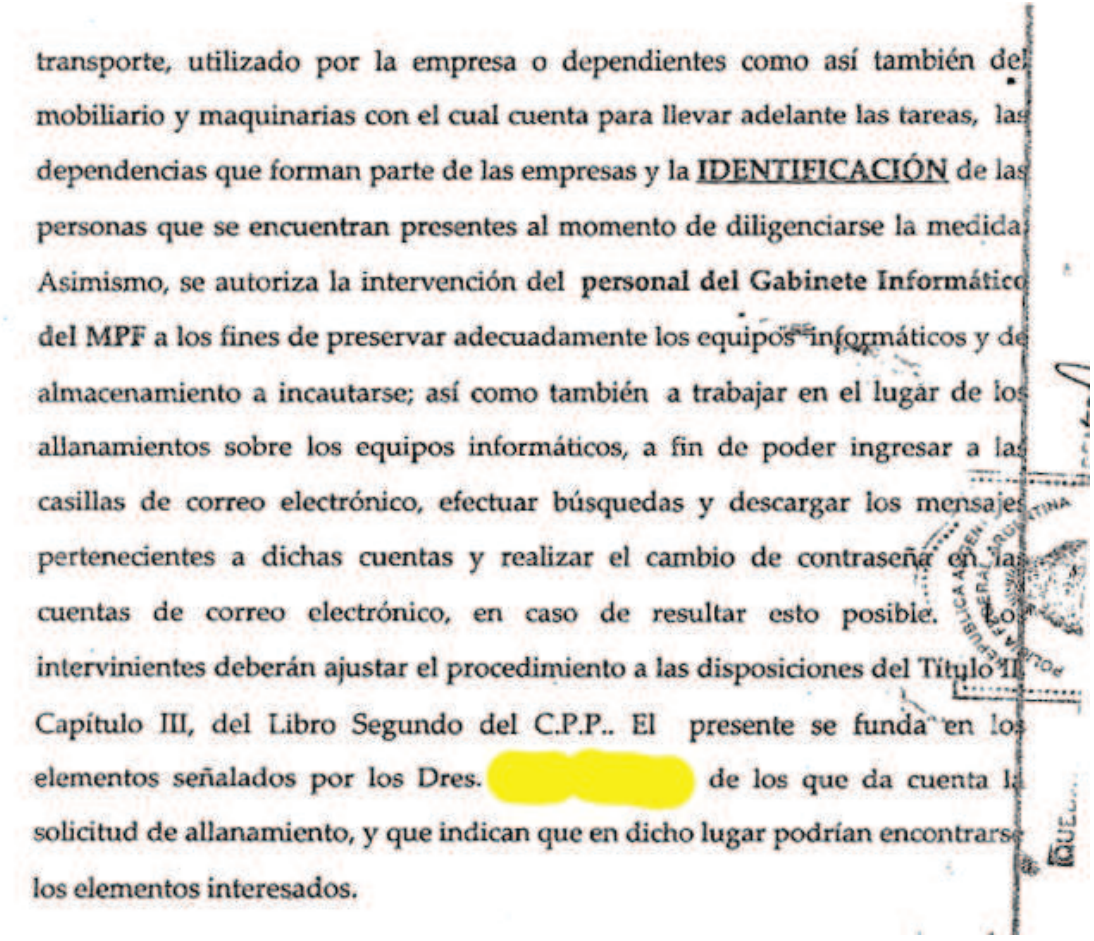
---

[417] Guide to Obtaining Communication Service Provider Evidence from the United States, United Nations, Url: http://www.un.org/en/sc/ctc/docs/2015/CSP%20Guidance%202015.pdf

[418] Texto extraído de la versión de la Constitución de Estados Unidos traducida en url: https://www.constitutionfacts.com/content/constitution/files/usconstitution_spanish.pdf

5.9. Un caso de análisis práctico.

Con la finalidad de continuar bajando a la praxis judicial Para sumar un ejemplo más relacionado al tema de análisis, y sólo a fines ejemplificativos, acompañamos parte de una autorización de una medida de allanamiento, donde en su interior y como puede observarse, el Juez de Garantías autoriza al personal del Gabinete Informático del MPF a ingresar a las casillas de correo electrónico, efectuar búsquedas, descargar mensajes y realizar el cambio de contraseña en las cuentas de correo electrónico encontradas en los equipos de la organización objeto del allanamiento.



transporte, utilizado por la empresa o dependientes como así también del mobiliario y maquinarias con el cual cuenta para llevar adelante las tareas, las dependencias que forman parte de las empresas y la **IDENTIFICACIÓN** de las personas que se encuentran presentes al momento de diligenciarse la medida. Asimismo, se autoriza la intervención del **personal del Gabinete Informático del MPF** a los fines de preservar adecuadamente los equipos informáticos y de almacenamiento a incautarse; así como también a trabajar en el lugar de los allanamientos sobre los equipos informáticos, a fin de poder ingresar a las casillas de correo electrónico, efectuar búsquedas y descargar los mensajes pertenecientes a dichas cuentas y realizar el cambio de contraseña en las cuentas de correo electrónico, en caso de resultar esto posible. Los intervinientes deberán ajustar el procedimiento a las disposiciones del Título II, Capítulo III, del Libro Segundo del C.P.P.. El presente se funda en los elementos señalados por los Dres. [redacted] de los que da cuenta la solicitud de allanamiento, y que indican que en dicho lugar podrían encontrarse los elementos interesados.

A nuestro criterio, la citada autorización judicial, más allá del posible cuestionamiento por considerar que muchas de dichas medidas autorizadas no encuentran sustento legal dentro del Código Procesal Penal de Entre Ríos (Provincia de la cuál es este caso concreto).

Por un lado, es posible afirmar que el pedido de "*trabajar en el lugar sobre los equipos informáticos, previo a su secuestro, con el objeto de poder ingresar a las casillas de correo electrónico, efectuar búsquedas y descargar los mensajes pertenecientes a dicha cuenta, relacionados con el hecho investigado*" es impreciso, excesivo y podría afectar garantías constitucionales de personas no relacionadas a la investigación en curso, toda vez que en los equipos informáticos existentes en los domicilios autorizados, podrían contener múltiples cuentas de correos electrónicos, propiedad de personas indeterminadas que podrían no tener ningún tipo de vínculo relacionado a la causa que motiva la presente investigación y cuyos contenidos en nada aprovecharían a la investigación del hecho en cuestión.

Que, el acceso a los contenidos de una cuenta de correo electrónico supone el ámbito de afectación de la privacidad más invasivo de todos (a diferencia de los datos de abonado y datos de tráfico), exigiendo que su acceso sea sólo ante el caso de necesidad y presuponiendo que existen motivos fundados para tener una expectativa razonable de que en dichas casillas, se encontrarían elementos de interés para la causa.

Que, en relación a los datos de contenido no hay discusiones sobre que nos encontramos en presencia del nivel de afectación más profunda que podría pensarse a nivel jurídico, superando todas las barreras a la intimidad del titular, accediendo y conociendo sus comunicaciones, donde se supone que el Estado ha considerado indispensable, a los fines de la averiguación de la verdad de los hechos –y que no existe otra vía menos invasiva–, la necesidad de acceder y conocer el contenido de esas comunicaciones privadas. Que, en el caso concreto, la falta de identificación de las cuentas de correo electrónico (la identificación de las cuentas o bien, patrones que podrían conducir a tener cierta verosimilitud al respecto del interés que tendría para la causa), dificulta la argumentación sobre la "necesidad" de acceder a dichas comunicaciones por parte de la fiscalía, quedando todo lo anteriormente expuesto sobre el principio de necesidad, fuera de combate.

Que, la autorización de ingreso a cuentas de correo "indeterminadas", también no parece superar los análisis realizados desde los principios de proporcionalidad y necesidad, sino que más bien parece excesivo y arbitrario, ya que

no existió en el caso concreto justificación alguna sobre que existan indicios sobre que las cuentas de correos vinculadas a dichos equipos (que tranquilamente pueden ser cuentas personales @gmail o @hotmail por ejemplo) tengan indicios ciertos de contener elementos de interés para la causa.

Que, aún con la gravedad e imprudencia de la medida anteriormente referenciada, el juez de garantías no sólo se autoriza "en blanco" al acceso y descarga de cuentas de correos electrónicos, sino que además, se autoriza "al momento de diligenciar la medida se proceda al cambio de contraseña en las cuentas de correo electrónico", haciendo que la ilegitimidad de la medida autorizada, a nuestro criterio, sea aún más notoria.

Que, si bien este último pedido, se encuentra fundamentado bajo el razonamiento que "*ello permite resguardar la información que se encuentra en la casilla de correo electrónico, de modo que no pueda ser eliminado o modificado su contenido en forma remota por terceros desde otros dispositivos, y así preservar la información a efectos de ser posteriormente analizada. A modo de ejemplo y para mayor ilustración de V.S., sería como fajar o poner en resguardo un buzón a fin de que ningún tercero pueda adulterar lo que se encuentra dentro de él*".

Que, por un lado debe analizarse primero que las cuentas puedan ser de personas interesadas en la investigación. Y sin embargo, si este fundamento fuera cierto, no se comprende cuál sería la finalidad de acceder y descargarse el contenido "de interés" (que como se puede observar en otros puntos de este informe, en la práctica tampoco han quedado claro como se ha definido dicho interés), si en definitiva, el acceso a la cuenta está corolado con el cambio de contraseña de las cuentas accedidas. Si el fundamento de cambiar la contraseña es evitar que un tercero acceda a borrar información, entonces, ¿cuál sería el fundamento de previamente realizar las copias al momento del propio allanamiento? Ya que si en definitiva la fiscalía se está llevando copias exactas de los contenidos "de interés" (o de todos los contenidos de la cuenta, que fue en definitiva lo que se intentó realizar en la práctica), tornarían inútiles los fundamentos del segundo pedido.

En fin, el caso concreto es sólo una muestra de una investigación realizada en la República Argentina, donde se puede observar que no solamente se hace uso de medidas de investigación no reguladas en los respectivos cuerpos procesales, sino que además, su disposición no sostendría un análisis exhaustivo a la luz de los principios previamente desarrollados.

5.10. Conclusiones preliminares

Tenemos certeza que la persecución y condena de los delitos informáticos depende de un factor clave: conseguir la evidencia digital necesaria para poder probar ante el juez competente, la culpabilidad de una o más personas en su participación en dichos hechos delictivos.

Ahora bien, si bien el acceso a esta evidencia digital puede darse de diversas formas, es muy probable que en el marco de la mayor parte de las investigaciones penales (en su etapa preparatoria) sea necesario acudir a una serie de medidas de investigación que tengan por finalidad la obtención de esos elementos probatorios que le permitan a la Fiscalía, avanzar hacia la acusación.

Sobre este contexto, partimos de una base donde las investigaciones sobre delitos cibernéticos que llevan adelante las fiscalías y fuerzas de seguridad, requieren de una variada gama de técnicas de investigación adecuadas para esta forma delictiva.

5.10.1. ¿Medidas de prueba o medidas de injerencia?

En el capítulo V hemos pretendido, en la medida de nuestras posibilidades y considerando ya la amplitud de la problemática abordada, realizar un breve repaso que a nuestro juicio se tornaba fundamental previo a dar paso al relevamiento acerca de si tal o cuál medida de investigación se encuentra o no regulada.

Por ello, la inclusión de este capítulo tiene que ver con realizar un desarrollo académico preliminar, a modo de construcción de un marco teórico necesario para avanzar luego sobre el relevamiento y el análisis de las propias medidas de investigación en sí mismas.

Ahora bien, del desarrollo realizado en dicho capítulo, consideramos apropiado destacar algunos aspectos fundamentales.

Por un lado, destacar la diferencia entre las medidas de prueba y las medidas de injerencia. Es clave comprender que los medios probatorios en general, donde es aplicable el famoso principio de libertad probatoria, no tienen (o no deberían tener) un grado importante de afectación de derechos y garantías. La confusión radica en que, en algunas de estas opciones del sistema abierto, pueden dar lugar a la existencia de medidas de coerción.

A modo de ejemplo en el derecho penal clásico, un homicidio podría ser probado a través de una gran cantidad de medios probatorios. Desde testigos, pruebas de pólvora en las manos de una persona, hasta la ubicación por gps de un dispositivo celular, o la grabación de un sistema de videovigilancia (datos en el fondo). La diferencia está que, para obtener esos elementos probatorios, la fiscalía va a tener que echar mano, en algunos casos (como por ejemplo el acceso al dispositivo celular del sospechoso) a medidas que afecten de una forma más concreta derechos y garantías consagradas constitucionalmente.

Por lo tanto, debemos tener claridad en comprender que siempre que exista una crisis o embate contra algún derecho o garantía de una persona, estaremos ante la presencia de una medida de coerción o de injerencia.

5.10.2. ¿Regular o no regular?

Continuando con el contexto del punto anterior, nuestra postura es clara en relación a que todas las medidas o técnicas especiales de investigación que hemos analizado en esta tesis doctoral son, a todas luces, medidas de injerencia.

En consecuencia, entendemos y adherimos a la idea que la ejecución de dichas medidas sin su previa regulación en la normativa vigente, provoca una afectación directa al principio de *nulla coactio sine lege,* y por lo tanto, una afectación directa al principio de legalidad.

Como se ha desarrollado en el punto 5.5., un adecuado análisis del principio de *nulla coactio sine lege* implica primero, confirmar la existencia y el alcance de la medida de investigación y luego, confirmar si dicha norma ha sido dictada tanto en conformidad objetiva como subjetiva.

Volviendo a la pregunta que nos convoca, consideramos un contundente sí ante la respuesta de la necesidad de la regulación de herramientas en materia procesal penal que permitan fundamentar las medidas solicitadas y autorizadas judicialmente.

Entendemos que, provisoriamente y ante la inexistencia de una adecuación de los respectivos códigos procesales penales, el sistema de justicia tenga que realizar una interpretación forzada del principio de libertad probatoria, a fin de sostener algún tipo de andamiaje jurídico que le permita continuar adelante con las investigaciones en curso.

5.10.3. La relación entre la regulación normativa y la potencial afectación de derechos y garantías

Como hemos visto a lo largo de nuestro trabajo, en la actualidad siguen existiendo múltiples jurisdicciones que continúan trabajando en investigaciones penales con la falta de regulación o la regulación inadecuada de las medidas de investigación tendientes a la obtención de evidencia digital, podrían implicar graves afectaciones al respeto a los derechos y libertades individuales del ámbito digital.

Afirmamos el potencial toda vez que, es precisamente la regulación de las reglas procesales lo que determina los límites a la ejecución de dichas medidas, y es allí donde se hace imprescindible recordar la importancia de la aplicación de todos

los principios que hemos repasado en la sección 5.8: principio de especialidad, principio de idoneidad, principio de excepcionalidad, principio de necesidad y sobre todo, el principio de proporcionalidad.

Si bien podrían existir casos donde el correcto control por parte de un Juez o Jueza de Garantías permita suplir las deficiencias normativas en materia procesal penal, lo cierto es que todo dependerá del nivel de conocimiento de esa persona, sumado a su postura personal acerca de si corresponde o no su aplicación, en interpretaciones subjetivas de los principios antes referidos.

Como hemos visto en el caso práctico planteado sobre el final del Capítulo V, en la práctica, los deseos y fantasías de encontrar el santo grial probatorio por parte de la Fiscalía, lleva a un exceso en el pedido de medidas de investigación, que como sucedió en el caso concreto, terminan siendo confirmadas por un Juez de Garantías, dejando a las personas afectadas en una delicada situación de estar siendo objeto de injerencias graves, para casos donde los fundamentos .

Por lo tanto, consideramos y reafirmamos que, la mejor forma de brindar garantías para la protección de los derechos y garantías de todas las personas, facilitar el trabajo tanto de la Fiscalía como del poder jurisdiccional, así como dotar de igualdad de armas a la defensa penal, es a través de una regulación adecuada y minuciosa de todas las medidas o técnicas especiales de investigación.

Capítulo VI: Medidas o técnicas especiales de investigación

6.1. Introducción

Las investigaciones sobre delitos cibernéticos que emprenden las fuerzas del orden requieren una amalgama de las técnicas policiales tradicionales y de nuevas técnicas. Aunque se pueden lograr algunas acciones investigativas con las facultades tradicionales, muchas disposiciones procesales con un enfoque espacial y orientado a los objetos no se adaptan bien a otro que involucra el almacenamiento de datos electrónicos y flujos de datos en tiempo real.

Empezamos aquí a recorrer los últimos trayectos de nuestro trabajo, y habiendo hecho un esfuerzo por desarrollar en la medida de lo posible, un marco teórico que nos permita ahora sí avanzar sobre un análisis más concreto sobre las medidas de investigación reguladas en los países alcanzados.

Este capítulo pretende entonces inicialmente realizar un relevamiento y estudio de derecho comparado sobre todas las medidas de investigación reguladas en Argentina, Brasil, Colombia, México y España, intentando construir ciertas categorías dogmáticas que nos permitan un mayor nivel de organización en un tema tan complejo como el que nos convoca.

Debemos advertir una dificultad inicial relacionado a la existencia de normativa fragmentada de acuerdo al tipo de tradición jurídica de cada país. Como pasa en Argentina y México, con un sistema federal, donde encontramos por un lado un Código Procesal Penal Federal y a su vez, cada provincia o Estado, internamente tiene su propio Código Procesal Penal. En consecuencia, en estos países, relevaremos tanto las medidas identificadas a nivel federal, como aquellas a nivel interno en el caso de existir.

6.2. Estadísticas a nivel internacional

6.2.1. Estudio exhaustivo sobre el delito informático (UNODC 2013)[419]

El cuestionario del estudio (realizado a nivel mundial) hace referencia a diez medidas investigativas relacionadas con el delito cibernético, que van desde el cateo y el decomiso genérico hasta poderes especializados, como la preservación de datos informáticos.

Identificamos aquí los aspectos principales del estudio (que por su extensión, invitamos al lector a acceder al mismo) que consideramos de interés para nuestro objeto de estudio:

- Los países encuestados (a nivel mundial) reportaron con mayor frecuencia la existencia de poderes generales (no específicos en el área de la cibernética) para todas las diligencias investigativas.
- Varios países también se refirieron a una legislación específica para la cibernética, notablemente para asegurar una ágil preservación de los datos informáticos y la obtención de datos almacenados sobre el suscriptor. Muchos países reportaron una falta de poder legal para medidas novedosas, como los instrumentos remotos para los estudios forenses.
- En general, entre los criterios nacionales hay menos elementos básicos en común en relación con las facultades investigativas en el caso de los delitos cibernéticos que con la tipificación como delito de muchos actos cibernéticos. Independientemente de la forma legal de los poderes investigativos, todas las autoridades encuestadas usan el cateo y el decomiso para la apropiación física del equipo de cómputo y la captura de datos informáticos.
- Fuera de Europa, alrededor de un tercio de los países reportaron dificultades para conminar a terceros en una investigación para proveer información.

[419] NACIONES UNIDAS, "Estudio exhaustivo sobre el delito cibernético", 2013, Url: https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime_Study_Spanish.pdf

- Alrededor de tres cuartas partes de los países recurren a medidas investigativas especializadas, como la recopilación de datos en tiempo real, o una preservación agilizada de datos.
- Las medidas más intrusivas, como las que involucran la recopilación de datos en tiempo real o el acceso al contenido de los datos, suelen requerir umbrales de requisitos más elevados, como aportar evidencias de un acto grave o la demostración de una causa probable o una sospecha razonable.
- Las obligaciones legales nacionales y las políticas de retención y divulgación de datos del sector privado varían enormemente de país a país, de industria a industria y de un tipo de datos a otro. Los países reportaron con mayor frecuencia el uso de órdenes de tribunales para obtener evidencia de los proveedores de servicios. Sin embargo, en algunos casos los agentes de la ley pudieron obtener datos almacenados sobre los suscriptores, el tráfico e incluso contenidos, directamente.
- Las normas de derechos humanos especifican que las leyes deben ser suficientemente claras para dar un indicio adecuado de las circunstancias en las cuales las autoridades están facultadas para usar una medida investigativa, y que deben existir garantías adecuadas y efectivas contra el abuso.
- En su mayoría, los países reportaron tener algún sistema de protección de los derechos de privacidad en la legislación nacional, así como el rango de límites y salvaguardas en las investigaciones. Sin embargo, cuando las investigaciones son transnacionales, las divergencias en los niveles de protección hacen imprevisible el acceso de los agentes extranjeros a los datos, y dan lugar a posibles brechas jurisdiccionales en los regímenes de protección de la privacidad.
- Más del 90% de los países que respondieron al cuestionario han comenzado a establecer estructuras especializadas para la investigación de los delitos cibernéticos y de los delitos que generan evidencia electrónica. Sin embargo, en los países en desarrollo estas estructuras no tienen suficientes recursos y sufren de un déficit de capacidades.

- Los países con menores niveles de desarrollo cuentan considerablemente con menos policías especializados, alrededor de 0,2 por cada 100.000 usuarios de Internet a nivel nacional. El porcentaje es de dos a cinco veces mayor en los países más desarrollados.
- Se reportó que el 70% de los oficiales encargados de hacer cumplir la ley en los países menos desarrollados carecían de conocimientos y equipo informático, y tan solo la mitad de ellos recibía capacitación más de una vez al año.
- Una tercera parte de los países de las Américas reportaron que los recursos de los agentes de la ley para investigar el delito cibernético eran insuficientes.
- El estudio recibió respuestas, por ejemplo, de tan solo el 20% de los 50 países menos desarrollados del mundo.
- Todos los países que respondieron en África, y más del 80% de los países de las Américas, Asia y Oceanía reportaron que necesitaban asistencia técnica.
- El área citada con mayor frecuencia para la asistencia técnica fue la de las técnicas generales de investigación de delitos cibernéticos.
- De los países que requerían asistencia técnica, el 60% indicó que la necesitaban las agencias encargadas de hacer cumplir la ley.

A modo general, los resultados de este estudio confirman que las facultades procesales tradicionales pueden extenderse a situaciones cibernéticas, en muchos casos dicho enfoque puede también llevar a una incertidumbre legal y a que se cuestione la legalidad de la recopilación de pruebas y, por ende, de su admisibilidad.

Independientemente de la forma legal de los poderes investigativos, todas las autoridades encuestadas usan el cateo y el decomiso para la apropiación física del equipo de cómputo y la captura de datos informáticos. La mayoría de los países también usan requerimientos para obtener de los proveedores de servicios de Internet los datos almacenados en computadoras.

Otro aspecto que nos parece de interés destacar del estudio, es que refleja que la interacción entre los agentes de la ley y los proveedores de servicios de Internet es particularmente compleja. Afirman que "*Los proveedores de servicios tienen información sobre sus suscriptores, facturas, algunas bitácoras de conexión,*

información sobre su ubicación (como datos de la torre celular, en el caso de los proveedores de telefonía móvil), y el contenido de sus comunicaciones, todo lo cual puede representar evidencia electrónica vital de un delito. Las obligaciones legales nacionales y las políticas de retención y divulgación de datos del sector privado varían enormemente de país a país, de industria a industria y de un tipo de datos a otro. Los países reportaron con mayor frecuencia el uso de órdenes de tribunales para obtener evidencia de los proveedores de servicios. Sin embargo, en algunos casos los agentes de la ley pudieron obtener datos almacenados sobre los suscriptores, el tráfico e incluso contenidos, directamente. En ese sentido, las organizaciones del sector privado a menudo reportaron tanto una política primaria de exigir el debido proceso legal para divulgar los datos, como el cumplimiento voluntario de las solicitudes directas de los agentes de la ley en algunas circunstancias. Las relaciones informales entre los agentes de la ley y los proveedores de servicios, cuya existencia fue reportada en más de la mitad de los países encuestados, asiste el proceso de intercambio de información y desarrollo de confianza. Las respuestas señalaron que existe la necesidad de equilibrar la privacidad y el debido proceso, con la divulgación oportuna de evidencia, para garantizar que el sector privado no se convierta en un 'cuello de botella' en las investigaciones."

6.2.2. Informe sobre Cibercrimen (ONU 2018)

En un informe de 2018 dedicado a la regulación en Cibercrimen publicado por la Comisión de Prevención del Crimen y Justicia Criminal de Naciones Unidas[420], se puede observar las diferencias existentes entre los avances en la regulación penal de fondo en Cibercrimen, sobre la regulación sobre los aspectos procesales penales.

De acuerdo a este informe "*la legislación específica, consistente con los requisitos de los derechos humanos y el estado de derecho, es la base para las acciones de justicia criminal sobre cibercrimen y evidencia electrónica. Muchos gobiernos de todo el mundo han emprendido reformas legales durante los últimos cinco años, utilizando muchas veces la Convención de Budapest sobre*

[420] Cybercrime: the state of legislation: UN Commission for Crime Prevention and Criminal Justice, Side-event - Vienna International Centre, Tuesday, 15 May 2018, 9h00h – 9h50, Conference Room M3, Url:

Ciberdelincuencia como una guía. La aprobación de legislación sustantiva para tipificar como delito los delitos contra las computadoras y por medio de computadoras, así como las regulación de las facultades procesales para permitir la recopilación de pruebas electrónicas suelen ser el punto de partida para construir las capacidades de desarrollo. Se observa un progreso mensurable y se pueden extraer lecciones importantes de esta experiencia".

Ese progreso mensurable está basado en unas estadísticas que han realizado en relación al avance en los distintos continentes sobre la regulación penal en cibercrimen, tanto sobre derecho penal substantivo, como sobre las reglas de derecho procesal penal aplicables a la evidencia electrónica o digital.

Comparativamente, en estadísticas relacionadas al nivel de normativización entre la regulación del derecho penal de fondo y el derecho penal de forma, aquellas del primer grupo siempre son superiores a las segundas, toda vez que es normal que en el proceso de regulación primero se priorice la tipificación penal de la acción considerada como delictuosa, y posteriormente (y a veces demasiado posteriormente) se piensa sobre las regulaciones de ajuste o adaptación de las normas procesales penales necesarias para avanzar en la ejecución práctica de esas investigaciones penales que permitan combatir los delitos anteriormente tipificados.

Si bien el estudio es mucho más complejo, a los fines de este artículo sólo citaremos los datos publicados en relación a las normativas procedimentales sobre la evidencia electrónica, donde es posible observar que los países americanos se encuentran en tercer lugar sobre los 5 continentes, siendo Europa la referencia con los países de mayor desarrollo.

Como aspecto positivo, destacamos que es motivo de celebración el avance general en las regulaciones de materia procesal relativas a la evidencia electrónica, que es observable en todos los continentes al comparar los estudios de 2013 y 2018.



- **Limited progress regarding specific procedural powers – reliance on general powers – problem of safeguards**

Specific procedural powers		In January 2013		In January 2018	
	States	Largely in place		Largely in place	
All Africa	54	5	9%	10	19%
All Americas	35	5	14%	9	26%
All Asia	42	8	19%	13	31%
All Europe	48	31	65%	39	81%
All Oceania	14	1	7%	3	21%
All	**193**	**50**	**26%**	**74**	**38%**

El título del trabajo expuesto manifiesta que se observan avances limitados en materia de facultades procesales específicas -que en general, encuentran apoyo en facultades procesales más generales-, conservando aún problemas para salvaguardar los derechos y garantías.

En particular, en el caso de América, puede observarse la evolución existente entre 2013 y 2018. Mientras que en 2013 se ha encontrado regulación en materia procesal penal -en gran medida- en un 14% de los 35 Estados relevados, en el 2018 se ha casi duplicado, alcanzando un 26%, notando un interés y mejoría en el desarrollo de la regulación.

6.1. El desafío de la investigación compleja

En este punto del trabajo, nos parece adecuado para destacar el desafío de la comprensión de la complejidad de las investigaciones, o que dicho de otra manera, implica que ya no estamos ante la presencia de investigaciones unidireccionales o lineales (como hoy se puede pensar para algunos delitos comunes) sino que

estamos convencidos que para aumentar el nivel de eficacia de las investigaciones sobre el cibercrimen se requiere que dichas investigaciones sean más bien circulares o complejas.

Nos parece adecuado comenzar repasando algunos conceptos que con su clásica claridad nos explica el maestro Marcelo Riquert, donde explica la expansión de las técnicas de investigación. Como bien señala Riquert, "*los penalistas se encuentran divididos por un lado, quienes postulan la suficiencia del derecho penal clásico o tradicional —el derecho penal nuclear de la escuela de Frankfurt—. Por el otro, quienes afirman la necesidad de avanzar hacia un nuevo o moderno derecho penal, provisto de un desarrollo dogmático que adapte la teoría del delito aggiornándola a las necesidades de una realidad en la que el delito común —realizado por una persona física y que daña por lesión efectiva a un bien jurídico individual— convive con el delito no convencional —perpetrado por personas de existencia ideal o por el crimen organizado y que pone en peligro bienes jurídicos macrosociales—. El reconocimiento de un sector de conflictividad como no convencional —es decir, distinto, singular, particular, de excepción— tiene como uno de sus efectos directos en el ámbito procesal el operar como legitimante para la incorporación de excepciones al trámite normal. De otra manera, sería imposible alcanzar algún grado mínimo de eficacia. La premisa sería: no puede abordarse la investigación de lo no convencional con las mismas herramientas que fueron diseñadas para perseguir lo común. La sofisticación de la conflictividad demanda, impone, remedios excepcionales. A la vez, su gravedad justifica que se adopten algunas reglas que flexibilicen los principios que tradicionalmente rigen en materia de prueba o las facultades que se disponen para concretar una investigación sin apartamiento del baremo constitucional*".

Su claridad hace innecesaria cualquier tipo de comentario, así que sólo rescataremos lo que a nuestro criterio es trascendental tener en cuenta en aras de comprender la necesidad del desarrollo de las técnicas especiales de investigación: el cibercrimen es a todas luces un delito no convencional, que para peor, se va actualizando y modificando en su modus operandi constantemente, obligando a las

personas encargadas de su persecución, a capacitarse y a ser creativos a la hora de llevar adelante investigaciones que tengan alguna pretensión de eficacia.

En nuestra experiencia en la realización de capacitaciones a distintas fuerzas de seguridad en Argentina, observamos que suelen tener un pensamiento lineal en el sentido que las investigaciones hacen uso de medidas de investigación, que a posteriori (en el caso que tengamos éxito en la búsqueda) nos brindará como resultado y consecuencia, datos (evidencia digital) que nos permitiría encontrar al delincuente y avanzar hacia su condena.

Sin embargo, entendemos que esa lectura unidireccional hacia la obtención de la evidencia digital, no suele dar buenas resultados o al menos no tan regularmente, por lo que rápidamente suele caerse en una frustración al momento de abordar la investigación de muchos delitos informáticos de la actualidad (sobre todo, si son parte de una banda de cibercrimen).

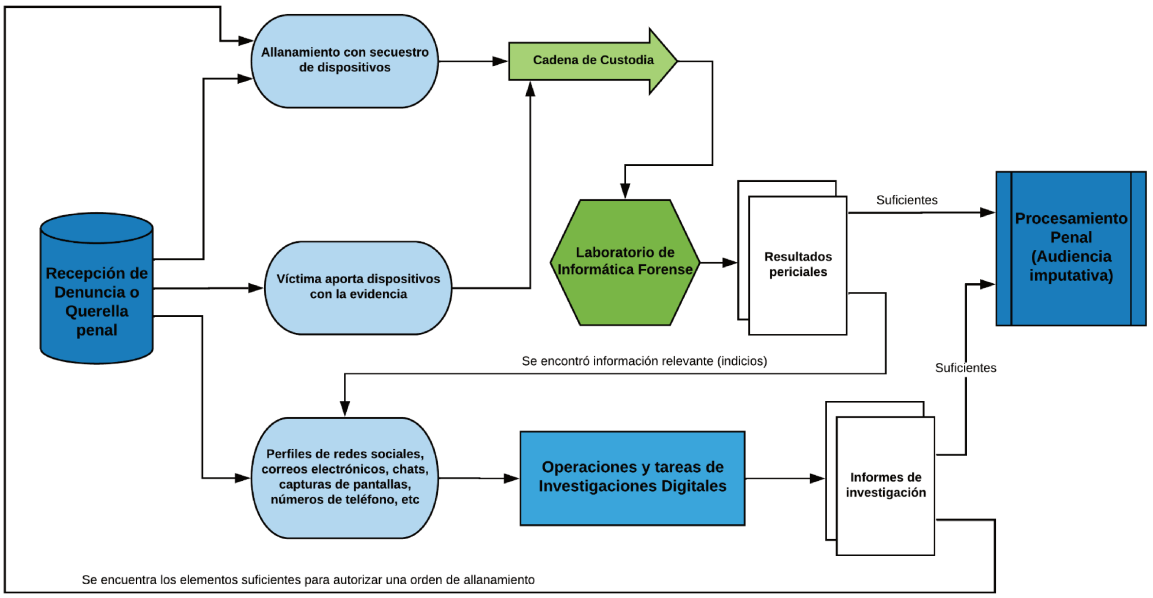
Es decir, debemos aprender a pensar que por un lado, podemos contar con evidencia digital desde un principio, sin siquiera haber ordenado una sola medida de investigación, por ejemplo, en los casos donde la víctima se acerca a la fiscalía y aporta evidencia digital que tiene en sus dispositivos electrónicos, o bien, la evidencia digital que será el eje de nuestra acusación, será posible conseguirla luego de un importante recorrido donde participará otra evidencia digital (en diferentes ciclos).

En las investigaciones convencionales, las investigaciones llevan su tiempo hasta lograr encontrar los fundamentos y se buscaba el momento adecuado para que el juez autorice el allanamiento domiciliario. Allí se secuestraba la información de interés, se peritaba y de allí (si teníamos suerte) teníamos los elementos para sostener la acusación.

Actualmente llegar a ese punto de la investigación en realidad puede no ser el fin, sino ser el comienzo de otra vuelta de investigación, toda vez que quizás de los datos extraídos de alguno de los dispositivos secuestrados, se obtuvo información relevante para continuar la investigación por otro lado (entendiendo que estamos en

la investigación de delitos complejos, que involucran varias personas, cierto nivel de profesionalización en la banda, etc.).

A continuación, compartimos un pequeño diagrama que expresa brevemente la idea que se intenta desarrollar.



A nuestro criterio, esta situación trae como consecuencia los actuales problemas en materia de análisis de información y sus correspondientes dictámenes periciales, donde al momento de solicitar la extracción, los pedidos son tan amplios y difusos, que culminan en la realización de una extracción forense (física o lógica) de la totalidad de los datos del teléfono móvil, enviando la totalidad de dichos datos a la fiscalía para su revisión (evitando así la realización de los dictámenes forenses que deberían realizarse desde el laboratorio forense).

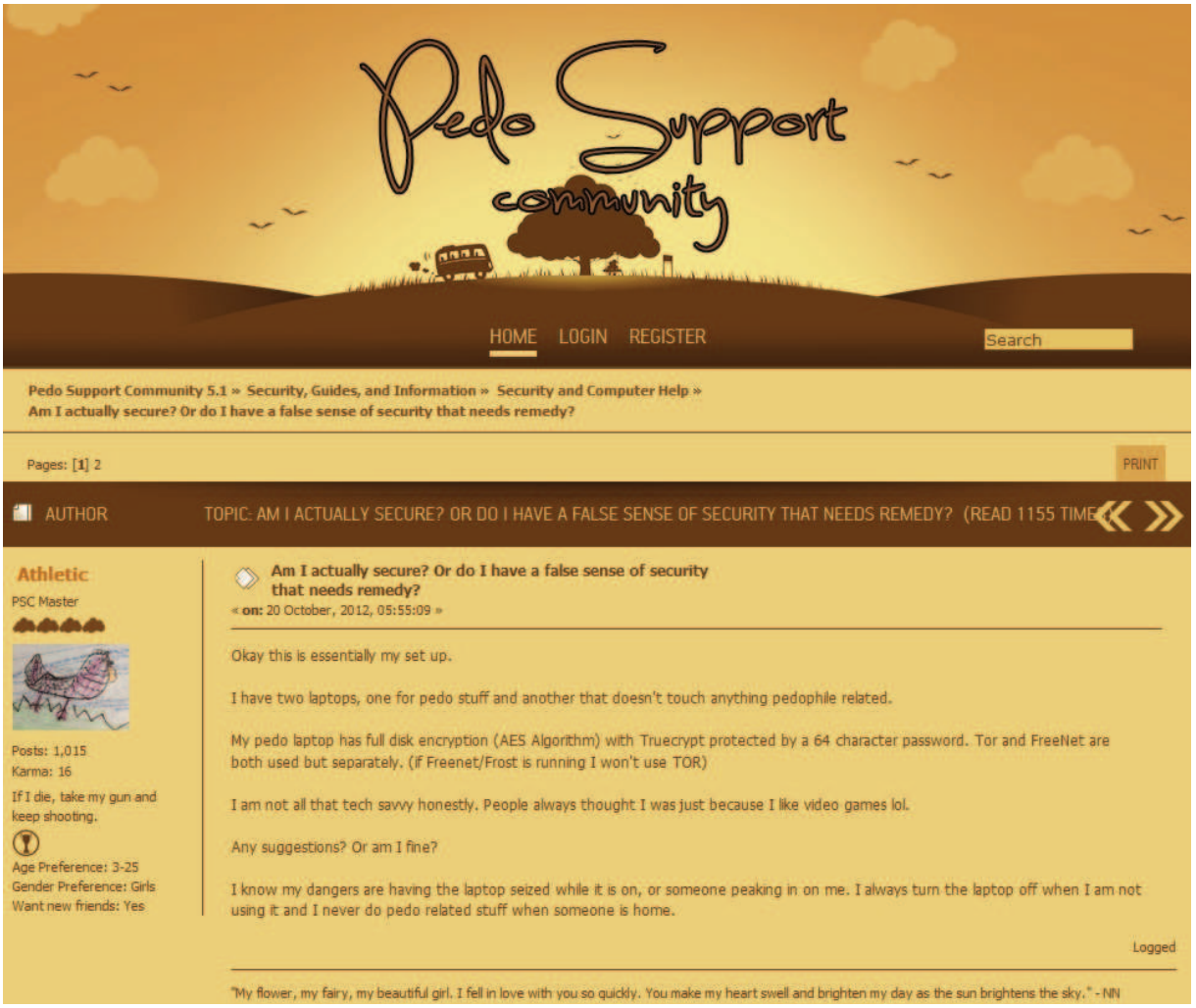
Si bien entendemos que en muchos casos esta situación puede tener como raíz la falta de recursos (falta de personal capacitado, falta de capacidad operativa en los laboratorios forenses, etc.), también es posible que otra de las razones sea que al momento de realizar dicha extracción forense, la fiscalía no tenga certeza acerca de qué datos podrían ser útiles para continuar con otras puntas de investigación.

Es decir, si desde el punto de vista lineal o unidireccional se intenta realizar preguntas concretas relacionadas a probar la culpabilidad de la persona investigada podría tener como resultado un dictamen negativo a los intereses de la fiscalía, sin embargo, si se aborda dicha información desde el punto de vista circular o complejo, quizás parte de esa información pueda llevar a otros rastros que hacen a la imagen más "grande" de la organización criminal.

A modo de ejemplo, en un caso de ransomware preguntarle al perito informático si en el equipo de la persona investigada se encuentra el código fuente, compilado o conversaciones con la víctima, podría tener resultados negativos. Sin embargo, si analizamos con la segunda postura, quizás se tenga que tener una visión más amplia que permita por ejemplo analizar conversaciones con otras personas que involucren palabras relacionadas al mismo delito (como "decrypter"), o bien, analizar si existen semillas de billeteras (wallets) de criptomonedas, que podrían también vincularlo a la extorsión de otras víctimas aún no identificadas de la misma banda.

Entendemos entonces que la amplitud necesaria para esta segunda forma de investigación, podría traer inconvenientes a la hora de formularse como puntos periciales, adicionalmente de que en ese punto de la investigación, quizás aún no se están haciendo las preguntas "correctas" sobre el caso, ya que aún en esta etapa preliminar, se está intentando determinar el modus operandi de esa banda de cibercriminales.

Por otro lado, es necesario visibilizar el aumento en la existencia de adopción de técnicas "antirastreos" o "antiforenses", dificultando aún más la labor de las personas que llevan adelante la investigación. A modo de graficar un poco esta actividad, acompañamos un par de capturas (que ya tienen sus años, pero que aún así sirve para graficar como en el año 2012 ya existía este nivel de uso de las técnicas).



En la parte que nos interesa, este usuario consulta por la mejor forma de "protegerse", comentando que tiene dos notebooks, una con material de abuso sexual infantil y otra "limpia". Explica que tiene su notebook con cifrado completo (algoritmo AES) realizado con Truecrypt con una contraseña de 64 caracteres. Desde allí, navega utilizando FreeNet y Tor para conectarse.



Pedo_Otaku
Permanently Banned!
Community Hero
Posts: 382
Karma: 0
So long - and thanks for all the paranoia!
Age Preference: 5-12+
Gender Preference: Boys & Girls
Want new friends: No

Re: Am I actually secure? Or do I have a false sense of security that needs remedy?
« Reply #7 on: 15 December, 2012, 07:50:46 »

Quote from: Athletic on 22 October, 2012, 05:52:18

I read about tails but I felt I wouldn't do it right and it would just mess up or some shit. I might eventually but for now I just have fail windows. I might also get a secure linux OS but who knows.

I think I will stick to WiFi... not really worried about that. I don't have bluetooth on.

I have windows update but it is set to not update without my permission.

Another question: Is it okay that I went on TOR while it was encrypting?

You sound pretty secure, but might I suggest routing your TOR traffic through at least another proxy inside a Virtual Machine.

Will a VPN+ VM Hide My IP address
http://m3hjrfh4hlqc67gb.onion/forum/thread/718

I connect to these .onion pedo sites with at least one extra proxy on top of my Tor connection just to be safe.

Using a public unsecured Wifi or your neighbor's hacked WEP Wifi isn't a bad idea either, but make sure you don't use their connection so much that they become suspicious of you. Or better yet, hack into other people's computers and use them as your proxies in a Botnet network. Go for the first option. The second one is not very feasible unless you are uber computer saavy and uber paranoid, but I think some us would want to do that if we could.

Logged

I love kids, but I don't molest them because I am a pedophile and NOT a child molester.

Otro usuario responde diciendo que suena bastante segura la configuración que tiene, pero le recomienda que el tráfico de TOR sea realizado a través de una máquina virtual, con la finalidad de dejar aún menos rastros. Luego sugiere también la utilización de alguna VPN (Virtual Private Network), para ocultar aún más su verdadero punto de conexión a ese tipo de material.

A modo genérico diremos que las técnicas antirastreos son todas aquellas que se utilizan con la finalidad de evitar dejar rastros de las acciones realizadas por los delincuentes, imposibilitando o al menos dificultando el "trackeo" por parte de las fuerzas de seguridad. En cambio, las técnicas antiforenses, buscan que ante el caso que las fuerzas de seguridad obtuvieran los dispositivos (notebooks, celulares, discos rígidos, pen drives, etc.), la información que se encuentra en ellos no puedan ser accedidas o analizadas en el marco de una pericia informática, por ejemplo por contar con procesos como cifrado o de borrado seguro (Wiping).

Como se puede observar, es la existencia de un subforo especial dedicado a técnicas de seguridad de la información, donde se pueden leer consejos y recomendaciones para evitar ser identificados, implica una realidad que debemos tener presente al momento de dimensionar la complejidad del delito que estamos investigando.

A modo de cierre provisorio de este tema, entendemos que la complejidad del delito actual, requiere que las fuerzas de seguridad y fiscalías intervinientes tengan una capacitación continúa al respecto, que permita primero comprender el delito investigado para luego, intentar determinar cuáles serán las medidas de investigación más pertinentes para el caso concreto.

6.2. Medidas de Investigación sugeridas en instrumentos internacionales

Al igual que hemos hecho en el Capítulo 3 dedicado a la búsqueda de delitos informáticos tipificados, comenzaremos primero haciendo un relevamiento sobre las medidas de investigación reguladas en los instrumentos internacionales más importantes al momento de escribir estas líneas, para luego pasar a la búsqueda en los ordenamientos jurídicos internos de cada país del estudio.

En el Convenio de Cibercrimen de Budapest, dentro de la Sección 2, dedicada a Derecho Procesal, a partir del Título 2, se comienza a enumerar una serie de medidas de investigación que, a criterio de este importante instrumento internacional en la materia, serían esenciales que los Estados partes tengan regulados con la finalidad de poder llevar adelante las investigaciones sobre los delitos informáticos. A continuación, realizaremos un repaso por las medidas de investigación propuestas por el Convenio:

Medidas de investigación reguladas en el Convenio de Cibercrimen de Budapest		Proyecto (Septiembre 2023) de Convención Internacional Integral sobre la Lucha contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos
1	**Artículo 16. Conservación inmediata de datos informáticos almacenados** 1. Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para permitir a sus autoridades competentes ordenar o imponer de otro modo la conservación inmediata de datos electrónicos especificados, incluidos los datos	**Artículo 25. Conservación acelerada de almacenados [datos informáticos] [información digital]** 1. Cada Estado Parte adoptará las medidas legislativas y de otro tipo que sean necesarias para permitir a sus autoridades competentes ordenar u obtener de manera similar la preservación expedita de [datos informáticos]

Medidas de investigación reguladas en el Convenio de Cibercrimen de Budapest		Proyecto (Septiembre 2023) de Convención Internacional Integral sobre la Lucha contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos
	de tráfico, almacenados a través de un sistema informático, especialmente cuando haya razones para pensar que son particularmente susceptibles de pérdida o de modificación. 2. Los Estados adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para obligar a una persona a conservar y proteger la integridad de los datos --que se encuentran en su poder o bajo su control y respecto de los cuales exista un mandato previo de conservación en aplicación del párrafo precedente-- durante el tiempo necesario, hasta un máximo de 90 días, para permitir a las autoridades competentes obtener su comunicación. Los Estados podrán prever que dicho mandato sea renovado posteriormente. 3. Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para obligar al responsable de los datos o a otra persona encargada de conservarlos a mantener en secreto la puesta en ejecución de dichos procedimientos durante el tiempo previsto por su derecho interno. 4. Los poderes y procedimientos mencionados en el presente artículo deben quedar sometidos a los artículos 14 y 15.	[información digital] específicos, incluidos datos de tráfico, que hayan sido almacenados por medios de [un sistema informático] [un dispositivo de tecnología de la información y las comunicaciones], en particular cuando haya motivos para creer que [los datos informáticos son] [la información digital es] particularmente vulnerable a pérdida o modificación. 2. Cuando un Estado Parte dé efecto al párrafo 1 supra mediante una orden a una persona de preservar [datos informáticos] [información digital] especificados almacenados en posesión o control de esa persona, el Estado Parte adoptará las medidas legislativas y de otra índole que sean necesarias. Puede ser necesario obligar a esa persona a preservar y mantener la integridad de esos [datos informáticos] [información digital] durante un período de tiempo tan largo como sea necesario, hasta un máximo de noventa días, para permitir a las autoridades competentes solicitar su divulgación. . Un Estado Parte podrá disponer que dicha orden se renueve posteriormente. 3. Cada Estado Parte adoptará las medidas legislativas y de otro tipo que sean necesarias para obligar al custodio u otra persona que deba preservar los [datos informáticos] [la información digital] a mantener confidencial la ejecución de dichos procedimientos durante el período de tiempo previsto. en su legislación interna.
2	**Artículo 17. Conservación y divulgación inmediata de los datos de tráfico** 1. A fin de asegurar la conservación de los datos de tráfico, en aplicación del artículo 16, los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para: a. procurar la conservación inmediata de los datos de tráfico, cuando uno o más prestadores de servicio hayan participado en la transmisión de dicha comunicación; y b. asegurar la comunicación inmediata a la autoridad competente del Estado, o a una	**Artículo 26. Conservación acelerada y divulgación parcial de datos de tráfico** Cada Estado Parte adoptará, con respecto a los datos de tráfico que deban conservarse conforme a las disposiciones del artículo sobre la conservación acelerada de [datos informáticos] [información digital] almacenados, las medidas legislativas y de otra índole que sean necesarias para: a) Garantizar que esa preservación expedita de los datos de tráfico esté disponible independientemente de si uno o más proveedores de servicios participaron en la transmisión de esa comunicación; y b) Garantizar la rápida divulgación a la

Medidas de investigación reguladas en el Convenio de Cibercrimen de Budapest		Proyecto (Septiembre 2023) de Convención Internacional Integral sobre la Lucha contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos
	persona designada por dicha autoridad, de datos de tráfico suficientes para permitir la identificación de los prestadores de servicio y de la vía por la que la comunicación se ha transmitido. 2. Los poderes y procedimientos mencionados en el presente artículo deben quedar sometidos a los artículos 14 y 15.	autoridad competente del Estado Parte, o a una persona designada por esa autoridad, de una cantidad suficiente de datos de tráfico para permitir al Estado Parte identificar a los proveedores de servicios y la ruta a través de la cual se realizó la comunicación o la información indicada. transmitido.
3	**Artículo 18. Mandato de comunicación** 1. Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias a fin de habilitar a sus autoridades competentes para ordenar: a. a una persona presente en su territorio que comunique los datos informáticos especificados, en posesión o bajo el control de dicha persona, y almacenados en un sistema informático o en un soporte de almacenaje informático; y b. a un prestador de servicios que ofrezca sus prestaciones en el territorio del Estado firmante, que comunique los datos en su poder o bajo su control relativos a los abonados y que conciernan a tales servicios; 2. Los poderes y procedimientos mencionados en el presente artículo deben quedar sometidos a los artículos 14 y 15. 3. A los efectos del presente artículo, la expresión «datos relativos a los abonados» designa cualquier información, expresada en datos informáticos o de cualquier otro modo, poseída por un prestador de servicio y que se refiere a los abonados de sus servicios, así como a los datos de tráfico o relativos al contenido, y que permite establecer: a. el tipo de servicio de comunicación utilizado, las disposiciones técnicas adoptadas al respecto y el tiempo del servicio; b. la identidad, la dirección postal o	**Artículo 27. Orden de producción** Cada Estado Parte adoptará las medidas legislativas y de otra índole que sean necesarias para facultar a sus autoridades competentes para ordenar: a) Que una persona en su territorio presente [datos informáticos] [información digital] específicos en posesión o control de esa persona que [estén] [estén] almacenados en [un sistema informático] [un dispositivo de tecnología de la información y las comunicaciones] o un [medio de almacenamiento de datos informáticos] [información digital]; y (b) Un proveedor de servicios que ofrece sus servicios en el territorio del Estado Parte a presentar información de abonado relacionada con dichos servicios en posesión o control de ese proveedor de servicios.

Medidas de investigación reguladas en el Convenio de Cibercrimen de Budapest		Proyecto (Septiembre 2023) de Convención Internacional Integral sobre la Lucha contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos
	geográfica y el número de teléfono del abonado o cualquier otro número de acceso, los datos relativos a la facturación y el pago, disponibles por razón de un contrato o de un alquiler de servicio; c. cualquier otra información relativa al lugar donde se ubican los equipos de comunicación, disponible por razón de un contrato o de un alquiler de servicio.	
4	**Artículo 19. Registro y decomiso de datos informáticos almacenados** 1. Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias a fin de habilitar a sus autoridades competentes para registrar o acceder de un modo similar: a. a un sistema informático o a una parte del mismo, así como a los datos informáticos que están almacenados; y b. a un soporte de almacenamiento que permita contener datos informáticos en su territorio. 2. Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para procurar que, cuando sus autoridades registren o accedan de un modo similar a un sistema informático específico o a una parte del mismo, conforme al párrafo 1 (a), y tengan motivos para creer que los datos buscados se hallan almacenados en otro sistema informático o en una parte del mismo situado en su territorio, y que dichos datos son igualmente accesibles a partir del sistema inicial o están disponibles a través de ese primer sistema, dichas autoridades estén en condiciones de ampliar inmediatamente el registro o el acceso y extenderlo al otro sistema. 3. Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias a fin de habilitar a sus autoridades competentes para decomisar u obtener de un modo similar los datos informáticos cuyo acceso haya sido realizado en	**Artículo 28. Búsqueda e incautación de [datos informáticos] [información digital] almacenados** 1. Cada Estado Parte adoptará las medidas legislativas y de otra índole que sean necesarias para facultar a sus autoridades competentes para registrar o acceder de manera similar en el territorio de ese Estado Parte: (a) [Un sistema informático] [Un dispositivo de tecnología de la información y las comunicaciones], parte del mismo, y [datos informáticos] [información digital] almacenados en el mismo; y b) Un medio de almacenamiento de [datos informáticos] [información digital] en el que puedan almacenarse los [datos informáticos] [información digital] buscados. 2. Cada Estado Parte adoptará las medidas legislativas y de otro tipo que sean necesarias para garantizar que, cuando sus autoridades busquen o accedan de manera similar a un [sistema informático] [dispositivo de tecnología de la información y las comunicaciones] específico o parte de él, de conformidad con el párrafo 1 (a) del presente artículo, y tener motivos para creer que los [datos informáticos] [información digital] buscados están almacenados en otro [sistema informático] [dispositivo de tecnología de la información y las comunicaciones] o parte de él en su territorio, y dichos datos están lícitamente accesible desde o disponible para el sistema inicial, dichas autoridades deberán poder realizar rápidamente la búsqueda para obtener acceso a ese otro [sistema informático] [dispositivo de tecnología de la información y las comunicaciones].

Medidas de investigación reguladas en el Convenio de Cibercrimen de Budapest		Proyecto (Septiembre 2023) de Convención Internacional Integral sobre la Lucha contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos
	aplicación de los párrafos 1 o 2. Estas medidas incluyen las prerrogativas siguientes: a. decomisar u obtener de un modo similar un sistema informático o una parte del mismo o un soporte de almacenaje informático; b. realizar y conservar una copia de esos datos informáticos; c. preservar la integridad de los datos informáticos almacenados pertinentes; y d. hacer inaccesibles o retirar los datos informáticos del sistema informático consultado. 4. Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias a fin de habilitar a sus autoridades competentes para ordenar a cualquier persona, que conozca el funcionamiento de un sistema informático o las medidas aplicadas para proteger los datos informáticos que contiene, que proporcione todas las informaciones razonablemente necesarias, para permitir la aplicación de las medidas previstas en los párrafos 1 y 2. 5. Los poderes y procedimientos mencionados en el presente artículo deben quedar sometidos a los artículos 14 y 15.	3. Cada Estado Parte adoptará las medidas legislativas y de otro tipo que sean necesarias para facultar a sus autoridades competentes para incautar o proteger de manera similar [datos informáticos] [información digital] en su territorio a los que se haya accedido de conformidad con los párrafos 1 o 2. Estas medidas incluirán el poder de: a) Confiscar o asegurar de manera similar [un sistema informático] [un dispositivo de tecnología de la información y las comunicaciones] o parte del mismo, o un medio de almacenamiento [de datos informáticos] [información digital]; (b) Hacer y conservar copias de [esos datos informáticos] [esa información digital] en formato electrónico; c) Mantener la integridad de los [datos informáticos] [información digital] pertinentes almacenados; (d) Hacer inaccesibles o eliminar [esos datos informáticos] [esa información digital] en el [sistema informático] [dispositivo de tecnología de la información y las comunicaciones] al que se accede. 4. Cada Estado Parte adoptará las medidas legislativas y de otra índole que sean necesarias para facultar a sus autoridades competentes para ordenar a cualquier persona que tenga conocimiento del funcionamiento del [sistema informático] [dispositivo de tecnología de la información y las comunicaciones] de que se trate, la información y red de telecomunicaciones, o sus componentes, o medidas aplicadas para proteger los [datos informáticos] [información digital] en la misma, para proporcionar, según sea razonable, la información necesaria para permitir la adopción de las medidas mencionadas en los párrafos 1 a 3 de este artículo.
5	**Artículo 20. Recogida en tiempo real de datos de tráfico** 1. Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias a	**Artículo 29. Recopilación de datos de tráfico en tiempo real** 1. Cada Estado Parte adoptará las medidas legislativas y de otra índole que sean necesarias para facultar a sus

	Medidas de investigación reguladas en el Convenio de Cibercrimen de Budapest	Proyecto (Septiembre 2023) de Convención Internacional Integral sobre la Lucha contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos
	fin de habilitar a sus autoridades competentes para: a. recoger o grabar mediante la aplicación de medios técnicos existentes en su territorio; b. obligar a un prestador de servicios, en el ámbito de sus capacidades técnicas existentes, a i. recoger o grabar mediante la aplicación de medios técnicos existentes en su territorio, o ii. prestar a las autoridades competentes su colaboración y su asistencia para recopilar o grabar, en tiempo real, los datos de tráfico asociados a comunicaciones específicas transmitidas en su territorio a través de un sistema informático. 2. Cuando un Estado, en razón de los principios establecidos en su ordenamiento jurídico interno, no pueda adoptar las medidas enunciadas en el párrafo 1 (a), podrá, en su lugar, adoptar otras medidas legislativas o de otro tipo que estime necesarias para asegurar la recogida o la grabación en tiempo real de los datos de tráfico asociados a comunicaciones específicas transmitidas en su territorio mediante la aplicación de medios técnicos existentes en ese territorio. 3. Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para obligar a un prestador de servicios a mantener en secreto la adopción de las medidas previstas en el presente artículo, así como cualquier información al respecto. 4. Los poderes y procedimientos mencionados en el presente artículo deben quedar sometidos a los artículos 14 y 15.	autoridades competentes para: a) Recopilar o registrar, mediante la aplicación de medios técnicos en el territorio de ese Estado Parte; y (b) Obligar a un proveedor de servicios, dentro de su capacidad técnica existente: i) Recopilar o registrar, mediante la aplicación de medios técnicos en el territorio de ese Estado Parte; o (ii) Cooperar y ayudar a las autoridades competentes en la recopilación o registro de; datos de tráfico, en tiempo real, asociados con comunicaciones específicas en su territorio transmitidos por medio de [un sistema informático] [un dispositivo de tecnología de la información y las comunicaciones]. 2. Cuando un Estado Parte, debido a los principios de su ordenamiento jurídico interno, no pueda adoptar las medidas mencionadas en el párrafo 1 (a), podrá en su lugar adoptar medidas legislativas y de otro tipo que sean necesarias para garantizar la recopilación en tiempo real o registro de datos de tráfico asociados con comunicaciones específicas transmitidas en su territorio, mediante la aplicación de medios técnicos en ese territorio. 3. Cada Estado Parte adoptará las medidas legislativas y de otra índole que sean necesarias para obligar a un proveedor de servicios a mantener confidencial el hecho de la ejecución de cualquier facultad prevista en este artículo y cualquier información relacionada con ella.
6	**Artículo 21. Interceptación de datos relativos al contenido** 1. Los Estados firmantes adoptarán las medidas	**Artículo 30. Interceptación de datos de contenidos** 1. Cada Estado Parte adoptará las medidas legislativas y de otra índole que sean necesarias, en relación con

Medidas de investigación reguladas en el Convenio de Cibercrimen de Budapest		Proyecto (Septiembre 2023) de Convención Internacional Integral sobre la Lucha contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos
	legislativas o de otro tipo que se estimen necesarias a fin de habilitar a sus autoridades competentes respecto a infracciones consideradas graves conforme a su derecho interno para: a. recoger o grabar mediante la aplicación de medios técnicos existentes en su territorio; y b. obligar a un prestador de servicios, en el ámbito de sus capacidades técnicas existentes, a i. recoger o grabar mediante la aplicación de medios técnicos existentes en su territorio, o ii. prestar a las autoridades competentes su colaboración y su asistencia para recopilar o grabar, en tiempo real, los datos relativos al contenido de concretas comunicaciones en su territorio, transmitidas a través de un sistema informático. 2. Cuando un Estado, en razón de los principios establecidos en su ordenamiento jurídico interno, no pueda adoptar las medidas enunciadas en el párrafo 1 (a), podrá, en su lugar, adoptar otras medidas legislativas o de otro tipo que estime necesarias para asegurar la recogida o la grabación en tiempo real de los datos relativos al contenido de concretas comunicaciones transmitidas en su territorio mediante la aplicación de medios técnicos existentes en ese territorio. 3. Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para obligar a un prestador de servicios a mantener en secreto la adopción de las medidas previstas en el presente artículo, así como cualquier información al respecto. 4. Los poderes y procedimientos mencionados en el presente artículo deben quedar sometidos a los artículos 14 y 15.	una serie de delitos graves que determinará el derecho interno, para facultar a sus autoridades competentes para: a) Recopilar o registrar, mediante la aplicación de medios técnicos en el territorio de ese Estado Parte; y (b) Obligar a un proveedor de servicios, dentro de su capacidad técnica existente: i) Recopilar o registrar, mediante la aplicación de medios técnicos en el territorio de ese Estado Parte; o (ii) Cooperar y ayudar a las autoridades competentes en la recopilación o registro de; datos de contenido, en tiempo real, de comunicaciones específicas en su territorio transmitidos por medio de [un sistema informático] [un dispositivo de tecnología de la información y las comunicaciones]. 2. Cuando un Estado Parte, debido a los principios de su ordenamiento jurídico interno, no pueda adoptar las medidas mencionadas en el párrafo 1 (a), podrá en su lugar adoptar medidas legislativas y de otro tipo que sean necesarias para garantizar la recopilación en tiempo real o registro de datos de contenido en comunicaciones específicas en su territorio, mediante la aplicación de medios técnicos en ese territorio. 3. Cada Estado Parte adoptará las medidas legislativas y de otra índole que sean necesarias para obligar a un proveedor de servicios a mantener confidencial el hecho de la ejecución de cualquier facultad prevista en este artículo y cualquier información relacionada con ella.
	Artículo 29 - Conservación rápida de datos	**Artículo 42. Conservación acelerada de los bienes**

Medidas de investigación reguladas en el Convenio de Cibercrimen de Budapest		Proyecto (Septiembre 2023) de Convención Internacional Integral sobre la Lucha contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos
7	**informáticos almacenados** 1. Una Parte podrá solicitar a otra Parte que ordene o asegure de otra forma la conservación rápida de datos almacenados por medio de un sistema informático que se encuentre en el territorio de esa otra Parte, respecto de los cuales la Parte requirente tenga la intención de presentar una solicitud de asistencia mutua con vistas al registro o al acceso de forma similar, la confiscación o la obtención de forma similar, o la revelación de los datos. 2. En las solicitudes de conservación que se formulen en virtud del párrafo 1 se indicará: a. la autoridad que solicita dicha conservación; b. el delito objeto de investigación o de procedimiento penal y un breve resumen de los hechos relacionados con el mismo; c. los datos informáticos almacenados que deben conservarse y su relación con el delito; d. cualquier información disponible que permita identificar a la persona encargada de la custodia de los datos informáticos almacenados o la ubicación del sistema informático; e. la necesidad de la conservación, y f. que la Parte tiene la intención de presentar una solicitud de asistencia mutua para el registro o el acceso de forma similar, la confiscación o la obtención de forma similar o la revelación de los datos informáticos almacenados. 3. Tras recibir la solicitud de otra Parte, la Parte requerida tomará las medidas adecuadas para conservar rápidamente los datos especificados de conformidad con su derecho interno. A los efectos de responder a una solicitud, no se requerirá la doble tipificación penal como condición para proceder a la conservación. 4. Cuando una Parte exija la doble tipificación penal como condición para atender una solicitud de asistencia mutua para el registro o el acceso de forma similar, la confiscación o la obtención de forma similar	**almacenados. [datos informáticos] [información digital]** 1. Un Estado Parte podrá solicitar a otro Estado Parte que ordene u obtenga de otro modo la preservación expedita de los datos almacenados mediante [un sistema informático] [un dispositivo de tecnología de la información y las comunicaciones], ubicado dentro del territorio de ese otro Estado Parte y con respecto de los cuales el Estado Parte requirente tiene intención de presentar una solicitud de asistencia jurídica mutua en la búsqueda o acceso similar, incautación o obtención similar, o divulgación de los datos. 2. La solicitud de conservación presentada con arreglo al apartado 1 especificará: a) La autoridad que solicita la preservación; b) El delito objeto de investigación o proceso judicial y un breve resumen de los hechos conexos; c) Los [datos informáticos] [información digital] almacenados que deben conservarse y su relación con el delito; d) Cualquier información disponible que identifique al custodio de los [datos informáticos] [información digital] almacenados o la ubicación del [sistema informático] [dispositivo de tecnología de la información y las comunicaciones]; e) La necesidad de la conservación; f) Que el Estado Parte requirente tiene la intención de presentar una solicitud de asistencia judicial recíproca en la búsqueda o acceso similar, incautación o obtención similar, o divulgación de los [datos informáticos] [información digital] almacenados; g) En su caso, la necesidad de mantener confidencial la solicitud de conservación y no notificarla al usuario. 3. Al recibir la solicitud de otro Estado Parte, el Estado Parte requerido tomará todas las medidas apropiadas para preservar rápidamente los datos especificados de conformidad con su derecho interno. A los efectos de responder a una solicitud, no se requerirá la doble

	Medidas de investigación reguladas en el Convenio de Cibercrimen de Budapest	Proyecto (Septiembre 2023) de Convención Internacional Integral sobre la Lucha contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos
	o la revelación de datos almacenados, dicha Parte podrá reservarse, en relación con delitos distintos de los previstos con arreglo a los artículos 2 a II del presente Convenio, el derecho a denegar la solicitud de conservación en virtud del presente artículo en los casos en que tenga motivos para creer que la condición de la doble tipificación penal no podrá cumplirse en el momento de la revelación. 5. Asimismo, las solicitudes de conservación únicamente podrán denegarse si: a. la solicitud hace referencia a un delito que la Parte requerida considera delito político o delito relacionado con un delito político o b. la Parte requerida considera que la ejecución de la solicitud podría atentar contra su soberanía, seguridad, orden publico u otros intereses esenciales. 6. Cuando la Parte requerida considere que la conservación por si sola no bastará para garantizar la futura disponibilidad de los datos, o pondrá en peligro la confidencialidad de la investigación de la Parte requirente o causará cualquier otro perjuicio a la misma, informará de ello sin demora a la Parte requirente, la cual decidirá entonces si debe pese a ello procederse a la ejecución de la solicitud. 7. Las medidas de conservación adoptadas en respuesta a la solicitud mencionada en el párrafo 1 tendrán una duración mínima de sesenta días, con objeto de permitir a la Parte requirente presentar una solicitud de registro o de acceso de forma similar, de confiscación u obtención de forma similar, o de revelación de los datos. Cuando se reciba dicha solicitud, seguirán conservándose los datos hasta que se adopte una decisión sobre la misma.	incriminación como condición para otorgar dicha preservación. 4. Un Estado Parte que exija la doble incriminación como condición para responder a una solicitud de asistencia judicial recíproca en la búsqueda o acceso similar, incautación o obtención similar, o divulgación de [datos informáticos] [información digital] almacenados podrá, con respecto a delitos distintos de los tipificados de conformidad con esta Convención, se reserva el derecho de denegar la solicitud de conservación prevista en este artículo en los casos en que tenga motivos para creer que, en el momento de la divulgación, no podía cumplirse la condición de doble incriminación. 5. Podrá denegarse una solicitud de conservación por los motivos previstos en el artículo 40, apartado 21. 6. Cuando el Estado Parte requerido considere que la conservación no garantizará la disponibilidad futura de los datos o amenazará la confidencialidad o perjudicará de otro modo la investigación del Estado Parte requirente, informará de ello con prontitud al Estado Parte requirente, quien luego determinará si No obstante, la solicitud debe ejecutarse. 7. Cualquier conservación efectuada en respuesta a una solicitud hecha de conformidad con El párrafo 1 tendrá una duración no superior a noventa días, a fin de que el Estado Parte requirente pueda presentar una solicitud de registro o acceso similar, incautación o obtención similar, o divulgación de los datos. Tras la recepción de dicha solicitud, los datos se seguirán conservando en espera de una decisión sobre dicha solicitud. 8. Antes de que expire el límite de conservación previsto en el párrafo 7, el Estado Parte requirente podrá solicitar una prórroga del período de conservación, por no más de noventa días adicionales.
8	**Artículo 30 - Revelación rápida de datos conservados sobre el trafico**	**Artículo 43. Divulgación acelerada de datos de tráfico conservados**

	Medidas de investigación reguladas en el Convenio de Cibercrimen de Budapest	Proyecto (Septiembre 2023) de Convención Internacional Integral sobre la Lucha contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos
	1. Cuando, con motivo de la ejecución de una solicitud presentada de conformidad con el artículo 29 para la conservación de datos sobre el tráfico en relación con una comunicación específica, la Parte requerida descubra que un proveedor de servicios de otro Estado participó en la transmisión de la comunicación, la Parte requerida revelará rápidamente a la Parte requirente un volumen suficiente de datos sobre el tráfico para identificar al proveedor de servicios y la vía por la que se transmitió la comunicación. 2. La revelación de datos sobre el tráfico en virtud del párrafo 1 únicamente podrá denegarse si: a. la solicitud hace referencia a un delito que la Parte requerida considera delito político o delito relacionado con un delito político, o b. la Parte requerida considera que la ejecución de la solicitud podría atentar contra su soberanía, seguridad, orden público u otros intereses esenciales.	1. Cuando, en el curso de la ejecución de una solicitud formulada de conformidad con el artículo 42 para conservar datos de tráfico relativos a una comunicación específica, el Estado Parte requerido descubra que un proveedor de servicios de otro Estado Parte participó en la transmisión de la comunicación, el El Estado Parte requerido revelará rápidamente al Estado Parte requirente una cantidad suficiente de datos de tráfico para identificar al proveedor de servicios y la ruta a través de la cual se transmitió la comunicación. 2. La divulgación de datos de tráfico con arreglo al apartado 1 podrá denegarse por los motivos previstos en el artículo 40, apartado 21.
9	**Artículo 31 - Asistencia mutua en relación con el acceso a datos informáticos almacenados** 1. Una Parte podrá solicitar a otra Parte que registre o acceda de forma similar, confisque u obtenga de forma similar y revele datos almacenados por medio de un sistema informático situado en el territorio de la Parte requerida, incluidos los datos conservados en aplicación del artículo 29. 2. La Parte requerida dará respuesta a la solicitud aplicando los instrumentos internacionales, acuerdos y legislación mencionados en el artículo 23, así como de conformidad con otras disposiciones aplicables en el presente capítulo. 3. Se dará curso a la solicitud lo antes posible cuando: a. existan motivos para creer que los datos pertinentes están especialmente expuestos al riesgo de pérdida o modificación, o b. los instrumentos, acuerdos o legislación mencionados en el párrafo 2 prevean la cooperación rápida.	**Artículo 44. Asistencia jurídica mutua para acceder almacenados [datos informáticos] [información digital]** 1. Un Estado Parte podrá solicitar a otro Estado Parte que busque o acceda de manera similar, incaute o proteja de manera similar y divulgue datos almacenados por medio de [un sistema informático] [un dispositivo de tecnología de la información y las comunicaciones] ubicado dentro del territorio del Estado Parte requerido. , incluidos los datos que hayan sido conservados de conformidad con el artículo 42. 2. El Estado Parte requerido responderá a la solicitud mediante la aplicación de los instrumentos y leyes internacionales pertinentes a que se refiere el artículo 35, y de conformidad con otras disposiciones pertinentes de este capítulo. 3. La solicitud se responderá de forma expedita cuando: (a) Hay motivos para creer que los datos relevantes son particularmente vulnerables a pérdida o modificación; o (b) Los instrumentos, acuerdos y leyes a que se refiere el párrafo 2 prevean la cooperación acelerada.

Medidas de investigación reguladas en el Convenio de Cibercrimen de Budapest		Proyecto (Septiembre 2023) de Convención Internacional Integral sobre la Lucha contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos
10	**Artículo 32 - Acceso transfronterizo a datos almacenados, con consentimiento o cuando sean accesibles al publico** Una Parte podrá, sin autorización de otra Parte: a. tener acceso a datos informáticos almacenados accesibles al público (fuente abierta), independientemente de la ubicación geográfica de los mismos, o b. tener acceso a datos informáticos almacenados en otro Estado, o recibirlos, a través de un sistema informático situado en su territorio, si dicha Parte obtiene el consentimiento lícito y voluntario de la persona legalmente autorizada a revelárselos por medio de ese sistema informático.	**No se encontró regulación al respecto**
11	**Artículo 33 - Asistencia mutua para la obtención en tiempo real de datos sobre el tráfico** 1. Las Partes se prestarán asistencia mutua para la obtención en tiempo real de datos sobre el tráfico asociados a comunicaciones especificas en su territorio transmitidas por medio de un sistema informático. Con sujeción a lo dispuesto en el párrafo 2, dicha asistencia se regirá por las condiciones y procedimientos establecidos en el derecho interno. 2. Cada Parte prestará dicha asistencia como mínimo respecto de los delitos por los que se podría conseguir la obtención en tiempo real de datos sobre el tráfico en un caso similar en su país.	**Artículo 45. Asistencia jurídica mutua en la recogida en tiempo real de datos de tráfico** 1. Los Estados Partes se prestarán asistencia jurídica mutua en la recopilación en tiempo real de datos de tráfico asociados con comunicaciones específicas en su territorio transmitidos por medio de [un sistema informático] [un dispositivo de tecnología de la información y las comunicaciones]. Sin perjuicio de lo dispuesto en el párrafo 2, dicha asistencia se regirá por las condiciones y procedimientos previstos en la legislación interna. 2. Cada Estado Parte proporcionará dicha asistencia al menos con respecto a delitos penales para los cuales la recopilación en tiempo real de datos de tráfico estaría disponible en un caso interno similar. 3. La solicitud presentada de conformidad con el apartado 1 del presente artículo especificará: a) El nombre de la autoridad solicitante; b) Un resumen de los hechos principales y la naturaleza de la investigación, procesamiento o procedimiento judicial al que se refiere la solicitud; c) Los [datos informáticos] [información digital] respecto de los cuales se requiere la recopilación de datos de tráfico y su relación con el delito u otro acto ilegal;

Medidas de investigación reguladas en el Convenio de Cibercrimen de Budapest		Proyecto (Septiembre 2023) de Convención Internacional Integral sobre la Lucha contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos
		(d) Cualquier dato disponible que identifique al propietario o usuario de los datos o la ubicación del [sistema informático] [dispositivo de tecnología de la información y las comunicaciones]; e) Justificación de la necesidad de recopilar datos sobre el tráfico; f) El período durante el cual se van a recoger datos de tráfico y la correspondiente justificación de su duración.
12	**Artículo 34 - Asistencia mutua relativa a la interceptación de datos sobre el contenido** Las Partes se prestarán asistencia mutua para la obtención o grabación en tiempo real de datos sobre el contenido de comunicaciones específicas transmitidas por medio de un sistema informático, en la medida en que lo permitan sus tratados y el derecho interno aplicables.	**Artículo 46. Asistencia jurídica mutua en el interceptación de datos de contenido** Los Estados Partes se prestarán asistencia jurídica mutua en la recopilación o registro en tiempo real de datos de contenido de comunicaciones específicas transmitidas por medio de [un sistema informático] [un dispositivo de tecnología de la información y las comunicaciones], en la medida permitida por los tratados aplicables a ellos y en virtud de sus leyes internas.

Tabla Nº 20: Cuadro comparativo sobre medidas de investigación reguladas entre el Convenio de Cibercrimen de Budapest y el Proyecto de Convención de ONU

En primer lugar, lo más importante a hacer notar como resultado del cuadro comparativo es la similitud existente entre las medidas de investigación reguladas por ambos instrumentos internacionales. Con la ventaja para el Convenio de Cibercrimen de Budapest, en que es un instrumento generado en el año 2001, y que aún con más de 22 años encima al momento de escribir estas líneas, puede observarse que el nuevo Proyecto de Convención de la ONU, prácticamente regula las mismas medidas de investigación, y sobre todo, con casi la mismas estructuras, por lo que pareciera ser evidente que han tomado de referencia lo regulado por Budapest.

Lo que también llama la atención, es que el Proyecto de ONU no ha incluído medidas similares a las reguladas en el Segundo Protocolo Adicional a la Convención de Budapest, aspecto que podría haber sido tenido en consideración.

A los fines de esta búsqueda e identificación de las medidas de investigación principales utilizadas en materia de cibercrimen, a continuación retomamos las dos herramientas principales que incorpora el Segundo Protocolo Adicional a la Convención de Cibercrimen de Budapest.

Medidas de investigación reguladas en el Segundo Protocolo Adicional del Convenio de Cibercrimen de Budapest	
13	**Artículo 6 - Solicitud de información sobre el registro de nombres de dominio** 1. Cada Parte adoptará las medidas legislativas y de otra índole que sean necesarias para facultar a sus autoridades competentes, a efectos de investigaciones o procedimientos penales específicos, para emitir una solicitud a una entidad que preste servicios de registro de nombres de dominio en el territorio de otra Parte para obtener la información que esté en posesión o bajo el control de la entidad, con el fin de identificar o ponerse en contacto con el titular de un nombre de dominio. 2. Cada Parte adoptará las medidas legislativas y de otra índole que sean necesarias para permitir que una entidad en su territorio divulgue dicha información en respuesta a una solicitud en virtud del párrafo 1, sujeto a las condiciones razonables previstas en la legislación nacional. 3. La solicitud en virtud del párrafo 1 deberá incluir: a. la fecha de emisión de la solicitud, y la identidad y los datos de contacto de la autoridad competente que emite la solicitud; b. el nombre de dominio sobre el que se solicita información y una lista detallada de la información solicitada, incluidos los elementos de datos concretos; c. una declaración en la que se indique que la solicitud se emite en virtud del presente Protocolo, que la necesidad de la información se debe a su pertinencia para una investigación o procedimiento penal específico y que la información sólo se utilizará para esa investigación o procedimiento penal específico, y d. el periodo de tiempo y la forma en que se divulgará la información y cualquier otra instrucción especial de procedimiento. 4. Si es aceptable para la entidad, una Parte podrá presentar una solicitud en virtud del párrafo 1 en formato electrónico. Es posible que se requieran niveles adecuados de seguridad y autentificación. 5. En caso de falta de cooperación por parte de una entidad descrita en el párrafo 1, la Parte requirente podrá pedir a la entidad que explique la razón por la que no divulga la información solicitada. La Parte requirente podrá solicitar consultas con la Parte en la que se encuentre la entidad, con miras a determinar las medidas disponibles para obtener la información. 6. Cada Parte, en el momento de la firma del presente Protocolo o del depósito de su instrumento de ratificación, aceptación o aprobación, o en cualquier otro momento, comunicará al Secretario General del Consejo de Europa la autoridad designada para los fines de consulta en virtud del párrafo 5. 7. El Secretario General del Consejo de Europa establecerá y mantendrá actualizado un registro de las autoridades designadas por las Partes con arreglo al párrafo 6. Cada Parte se asegurará de que los datos que haya facilitado para el registro sean correctos en todo momento.

14	**Artículo 7 - Divulgación de la información de los abonados** 1. Cada Parte adoptará las medidas legislativas y de otra índole que sean necesarias para facultar a sus autoridades competentes para emitir una orden que se presentará directamente a un proveedor de servicios en el territorio de otra Parte, a fin de obtener la divulgación de información especificada y almacenada del abonado que esté en posesión o bajo el control de dicho proveedor de servicios, cuando la información sobre el abonado sea necesaria para las investigaciones o procedimientos penales específicos de la Parte emisora. 2 a. Cada Parte adoptará las medidas legislativas y de otra índole que sean necesarias para que un proveedor de servicios en su territorio divulgue información sobre los abonados en respuesta a una orden en virtud del párrafo 1. b. En el momento de la firma del presente Protocolo o al depositar su instrumento de ratificación, aceptación o aprobación, una Parte podrá – con respecto a las órdenes emitidas a los proveedores de servicios en su territorio – hacer la siguiente declaración: "La orden en virtud del párrafo 1 del artículo 7 debe ser emitida por un fiscal u otra autoridad judicial, o bajo su supervisión, o de lo contrario ser emitida bajo una supervisión independiente". 3. La orden a que se refiere el párrafo 1 deberá especificar: a. la autoridad emisora y la fecha de emisión; b. una declaración de que la orden se emite en virtud del presente Protocolo; c. el nombre y la dirección del proveedor o proveedores de servicios que deben ser notificados; d. el delito o delitos que son objeto de la investigación o el procedimiento penal; e. la autoridad que solicita la información específica sobre el abonado, si no es la autoridad emisora, y f. una descripción detallada de la información específica sobre el abonado que se busca. 4. La orden con arreglo al párrafo 1 irá acompañada de la siguiente información complementaria: a. los fundamentos jurídicos internos que facultan a la autoridad para emitir la orden; b. una referencia a las disposiciones legales y a las sanciones aplicables al delito objeto de investigación o enjuiciamiento; c. la información de contacto de la autoridad a la que el proveedor de servicios deberá devolver la información del abonado, a la que podrá solicitar más información o a la que responderá de otro modo; d. el periodo de tiempo para devolver la información del abonado y la forma de devolverla; e. si ya se ha solicitado la conservación de los datos, incluida la fecha de conservación y cualquier número de referencia aplicable; f. cualquier instrucción procesal especial; g. si procede, una declaración de que se ha realizado una notificación simultánea de conformidad con el párrafo 5, y h. cualquier otra información que pueda facilitar la obtención de la divulgación de la información del abonado. 5...Nota del Autor: (se excluye por regular aspectos de forma del Protocolo y no relativas a la medida de investigación de interés).

Tabla Nº 21: Resumen de medidas de investigación adicionadas por el Segundo Protocolo Adicional del Convenio de Cibercrimen de Budapest.

Si bien entendemos que este Segundo Protocolo Adicional regula estas dos medidas, a nuestro criterio ambas han sido diseñadas desde el espíritu de cooperación internacional que trae consigo el propio Convenio de Cibercrimen de Budapest, ya que como podemos observar en los textos de las mismas, ambas regulan las formas (y límites) que deberán tenerse en cuenta para solicitar información de nombres de dominio o de abonados a otros Estados miembros.

Por lo expuesto anteriormente, y considerando que la búsqueda y alcance de la presente tesis tiene una orientación de búsqueda de regulación de medidas de investigación a nivel interno, es decir, que cada Estado Parte debería tener reguladas (o sería positivo que las tuviera) a fin de poder contar con herramientas jurídicas para agilizar las investigaciones en curso. Por este motivo, consideramos apropiado excluir de nuestra selección de medidas de investigación básicas a las dos medidas agregadas por el Segundo Protocolo Adicional.

Dicho esto, las medidas de investigación propuestas por el Convenio de Budapest (entendiendo que el proyecto de ONU no incorpora ninguna medida distinta) a fin de que sean reguladas e incorporadas a los ordenamientos internos de cada Estado, serían las siguientes:

Nº	Medidas de investigación reguladas en el Convenio de Cibercrimen de Budapest
1	Conservación inmediata de datos informáticos almacenados (Artículo 16)
2	Conservación y divulgación inmediata de los datos de tráfico (Artículo 17)
3	Mandato de comunicación (Artículo 18)
4	Registro y decomiso de datos informáticos almacenados (Artículo 19)
5	Recogida en tiempo real de datos de tráfico (Artículo 20)
6	Interceptación de datos relativos al contenido (Artículo 21)
7	Conservación rápida de datos informáticos almacenados (Art. 29)
8	Revelación rápida de datos conservados sobre el tráfico (Art. 30)
9	Asistencia mutua en relación con el acceso a datos informáticos almacenados (Art. 31)

10	Acceso transfronterizo a datos almacenados, con consentimiento o cuando sean accesibles al público (Art. 32)
11	Asistencia mutua para la obtención en tiempo real de datos sobre el tráfico (Art. 33)
12	Asistencia mutua relativa a la interceptación de datos sobre el contenido (Art. 34)
13	Solicitud de información sobre el registro de nombres de dominio (Art. 6 SPA)
14	Divulgación de la información de los abonados (Art. 7 SPA)

Tabla Nº 22: Resumen de medidas de investigación reguladas por el Convenio de Cibercrimen de Budapest.

Una primer clasificación que nos parece pertinente de realizar, a fines de evitar la duplicación de medidas, consiste en separar aquellas medidas que puedan ser exigibles a través del poder de coerción de un Estado dentro de su territorio, de aquellas medidas de cooperación, que pretendan lograr la misma medida de investigación pero sobre datos que se encuentre en territorio de otro Estado parte (o incluso, de otro Estado que no forme parte del Convenio).

De acuerdo a esta clasificación, podríamos entonces distinguir la existencia de 8 medidas de investigación que pueden ser aplicadas dentro del propio territorio, vs. 6 medidas de investigación que han sido pensadas para los pedidos de cooperación internacional.

Nº	Medidas de investigación reguladas en el Convenio de Cibercrimen de Budapest categorizadas de acuerdo a la posibilidad de aplicación dentro del territorio del Estado Parte
1	Conservación inmediata de datos informáticos almacenados (Artículo 16)
2	Conservación y divulgación inmediata de los datos de tráfico (Artículo 17)
3	Mandato de comunicación (Artículo 18)
4	Registro y decomiso de datos informáticos almacenados (Artículo 19)
5	Recogida en tiempo real de datos de tráfico (Artículo 20)
6	Interceptación de datos relativos al contenido (Artículo 21)

Tabla Nº 23: Resumen de medidas de investigación reguladas por el Convenio de Cibercrimen de Budapest, categorizadas de acuerdo a la posibilidad de aplicación dentro del territorio del Estado Parte.

Nº	Medidas de investigación reguladas en el Convenio de Cibercrimen de Budapest categorizadas de acuerdo a la posibilidad de aplicación fuera del territorio del Estado Parte
1	Conservación rápida de datos informáticos almacenados (Art. 29)
2	Revelación rápida de datos conservados sobre el tráfico (Art. 30)
3	Asistencia mutua en relación con el acceso a datos informáticos almacenados (Art. 31)
4	Acceso transfronterizo a datos almacenados, con consentimiento o cuando sean accesibles al público (Art. 32)
5	Asistencia mutua para la obtención en tiempo real de datos sobre el tráfico (Art. 33)
6	Asistencia mutua relativa a la interceptación de datos sobre el contenido (Art. 34)
7	Solicitud de información sobre el registro de nombres de dominio (Art. 6 SPA)
8	Divulgación de la información de los abonados (Art. 7 SPA)

Tabla Nº 24: Resumen de medidas de investigación reguladas por el Convenio de Cibercrimen de Budapest, categorizadas de acuerdo a la posibilidad de aplicación fuera del territorio del Estado Parte.

Como primera observación que podemos realizar, es que son más las medidas sugeridas que tienen que ver con la obtención de información en otro país Parte, que las medidas sugeridas para la obtención dentro del propio país. Entendemos que esto es así debido a que uno de los objetivos principales del Convenio de Budapest es precisamente establecer lazos de cooperación más ágiles entre los países parte.

Realizada esta primer clasificación, y previo al avance en el relevamiento de otras medidas de investigación reguladas en los países objeto del estudio, consideramos apropiado realizar al menos una breve descripción y desarrollo de cada una de las medidas de investigación sugeridas para implementar dentro del territorio del país, excluyendo aquellas que tengan que ver con la cooperación

internacional, aspecto que por su complejidad y profundamente, dejaremos fuera del alcance de esta tesis.

6.2.1. Conservación rápida de datos informáticos almacenados

Esta medida tiene por objeto garantizar que las autoridades nacionales competentes puedan ordenar u obtener de manera similar la conservación rápida de datos informáticos específicos almacenados en el marco de una investigación o procedimiento penal específico.

La "conservación" requiere que los datos, que ya existen y están almacenados de alguna forma, sean protegidos contra todo lo que pudiera causar que su calidad o condición actual sufriera un cambio o deterioro. Requiere que sean guardados a salvo de toda modificación, deterioro o eliminación. La conservación no significa necesariamente que los datos sean "congelados" (es decir, sean inaccesibles) y que los mismos, o copias de los mismos, no puedan ser utilizados por sus legítimos usuarios. La persona a quien va dirigida la orden podría, en función de las especificaciones exactas de la orden, seguir accediendo a los datos. De hecho, el artículo 16 del Convenio de Budapest donde se regula esta medida, no especifica la manera en que han de conservarse los datos. Queda a criterio de cada Parte determinar la manera de conservación apropiada y, en los casos en que proceda, si la conservación de los datos debiera también llevar a su "congelación".

Por otro lado, la referencia a "ordenar o imponer de otra manera" tiene como finalidad permitir el uso de otros métodos jurídicos para lograr la conservación además de una orden judicial o administrativa o de una directiva (por ejemplo, de la policía o el fiscal). El derecho procesal de algunos Estados no contempla las órdenes de conservación, por lo que la conservación y obtención de los datos requiere una orden de registro y confiscación, o de presentación de información. El uso de la frase "o imponer de otra manera" ofrece cierta flexibilidad a los Estados para que apliquen este artículo empleando estos medios.

El poder para ordenar o imponer de otra manera la conservación rápida de datos electrónicos específicos se aplica a todo tipo de datos informáticos almacenados. Ello puede incluir cualquier tipo de datos que estén especificados en

la orden de conservación de datos. Sin embargo, al momento de su regulación, han incluído que las Partes "*deben establecer medidas que se utilizarán en particular cuando existan razones para creer que dichos datos son especialmente susceptibles de pérdida o de modificación*."

Ello puede incluir situaciones en que los datos sean objeto de un breve período de conservación, tal como ocurre cuando una empresa tiene la política de eliminar los datos después de un cierto período de tiempo, o cuando los datos son borrados habitualmente cuando se utiliza el dispositivo de almacenamiento para grabar otros datos. También puede referirse a la naturaleza de quien custodia los datos o a la manera insegura en que se almacenan los datos. Sin embargo, si quien los custodia no fuera una institución confiable (difícil categorización), desde las fiscalías sería más seguro lograr su conservación mediante registro y confiscación, en lugar de enviar una orden que podría no ser obedecida, o bien, podrían presentarse argumentos técnicos de muy difícil comprobación a nivel pericial.

Nos parece de interés señalar que en el segundo párrafo se especifica que cuando una Parte imparta una orden de conservación de datos, dicha orden ha de ser en relación a "*determinados datos almacenados que se encuentren en poder o bajo el control de esa persona*". Es importante esta referencia ya que por lo general, en la actualidad las empresas suelen subcontratar los servicios de hosteo y procesamiento de datos, por lo que es muy probable que los datos en realidad puedan estar almacenados en otro lugar, aunque estando sujetos al control de esa persona (o empresa). Es decir, que alcanzaría también a los datos en poder de un proveedor de servicios de dicha empresa.

Como bien señala la Fiscal especializada Daniela Dupuy[421], "*el problema que existe cuando esta petición no está legislada o reglamentada es que el proveedor no tiene la obligación de responder al requerimiento del fiscal o juez y hasta podría avisar al infractor que lo están investigando. Entonces, el juez o el fiscal, quien se encuentre a cargo de la investigación, debería poder ordenar la conservación y prote*

[421] "Desafíos procesales en la investigación de delitos informáticos"

Por último, comentar que el párrafo 3 impone la obligación de mantener en secreto la ejecución de los procedimientos de conservación a la persona que custodia los datos o a otra persona encargada de su conservación durante el tiempo previsto en su derecho interno. Ello requiere que las Partes adopten medidas para garantizar el secreto respecto de la conservación rápida de los datos almacenados y fijen el límite de tiempo en que se debe mantener el secreto. Esta medida da cuenta de las necesidades de las autoridades encargadas de la aplicación de las leyes para que el sospechoso de la investigación no tenga conocimiento de la misma, al igual que del derecho a las personas al respeto de la vida privada. Para las autoridades encargadas de la aplicación de las leyes, la conservación rápida de los datos forma parte de las investigaciones iniciales, por lo que puede ser importante mantener el secreto en esa etapa.

Está claro que la conservación es una medida preliminar en espera de la adopción de otras medidas legales para la obtención o la revelación de los datos, por lo que lograr mantener el secreto es necesario para evitar que otras personas intenten alterar o borrar los datos.

6.2.2. Conservación y divulgación inmediata de los datos de tráfico

Como veníamos mencionando anteriormente, esta medida tiene una estrecha relación con lo que hemos desarrollado para la conservación rápida de los datos informáticos. La diferencia es que este artículo establece la revelación rápida de algunos datos sobre el tráfico con el fin de identificar a los proveedores de servicios que estuvieron involucrados en la transmisión de las comunicaciones especificadas.

Recordemos que el concepto de datos de tráfico y sus implicaciones jurídicas ya las hemos desarrollado en el capítulo anterior, dentro de la teoría de los 3 escalones (2do escalón).

La obtención de los datos sobre el tráfico almacenados correspondientes a comunicaciones pasadas puede ser esencial para determinar el origen o el destino de las comunicaciones realizadas, elemento crucial para identificar a las personas

que han distribuido, por ejemplo, material de abuso sexual infantil, información fraudulenta, malware, o que han intentado acceder o han accedido ilegalmente a sistemas informáticos, ya sea a los datos contenidos en el sistema o a su correcto funcionamiento.

Sin embargo, debemos destacar que la razón de esta especial medida tiene que ver con que en muchos casos esos datos se almacenan sólo por cortos períodos de tiempo; si es que se almacenan, ya que la cantidad de información puede ser inmensa. Como también ya hemos desarrollado, hasta hace no muchos años muchos países europeos tenían normativas que obligaban a la guarda o retención de datos de tráfico por un tiempo determinado (por ejemplo, por dos años), normativa que ya fue declarada inconstitucional.

Sea cual fuera la razón, puede ser vital para el marco de una investigación acceder a este tipo de información, por eso es importante que se tomen medidas de conservación destinadas a garantizar la integridad de esos datos.

En muchos casos puede estar involucrado en la transmisión de una comunicación más de un proveedor de servicios. Es decir, que cada proveedor de servicios puede poseer algunos datos sobre el tráfico relacionados con la transmisión de una comunicación específica, que han sido generados y conservados por ese proveedor de servicios en relación con el tránsito de la comunicación por su sistema o que han sido aportados por otros proveedores de servicios. Algunas veces los datos sobre el tráfico, o al menos algunos tipos de datos sobre el tráfico, se comparten entre los proveedores de servicios involucrados en la transmisión de la comunicación con fines comerciales, de seguridad o técnicos. En tal caso, cualquiera de los proveedores de servicios puede poseer los datos sobre el tráfico que son esenciales para determinar el origen o el destino de la comunicación. Sin embargo, en muchos casos no hay ningún proveedor de servicios que posea la suficiente cantidad de datos esenciales relativos al tráfico para poder determinar el origen real o el destino de la comunicación. Cada uno posee una parte del rompecabezas, y es necesario examinar cada una de estas partes para identificar el origen o el destino de la comunicación (como puede suceder al realizar el seguimiento de una comunicación realizada a través de nodos de Tor).

Como los datos sobre el tráfico no son revelados a las autoridades encargadas de aplicar las leyes cuando se envía una orden de conservación de datos a un proveedor de servicios (sino que se obtienen o revelan sólo más tarde después de que se han tomado otras medidas jurídicas), las autoridades que llevan adelante la investigación no pueden saber si el proveedor de servicios posee todos los datos esenciales relativos al tráfico o si otros proveedores de servicios participaron en la transmisión de la comunicación. Por consiguiente, este artículo dispone que el proveedor de servicios que recibe una orden de conservación de datos, o una medida similar, deberá revelar con prontitud a las autoridades competentes, o a otra persona designada, un volumen suficiente de datos sobre el tráfico que permita a las autoridades competentes identificar tanto a los proveedores de servicios como el cauce por el cual se transmitió la comunicación.

Las autoridades competentes deberían especificar con claridad el tipo de datos sobre el tráfico que deben revelarse. La recepción de esa información permitiría a las autoridades competentes determinar si es necesario tomar medidas de conservación respecto de otros proveedores de servicios. De este modo, las autoridades encargadas de la investigación pueden rastrear la comunicación para determinar su origen o su destino, e identificar al autor, o autores, del delito concreto que se investiga.

Por último, diremos que si la regulación de esta medida por parte del Convenio de Budapest ha sido pensada o diseñada pensando en ISP que ya tienen guardados los datos de tráfico por alguna razón (por obligación legal de su país, por política propia de la empresa, etc.) entendemos que nada obsta para que la misma medida pueda utilizarse para solicitar la guarda de datos hacia el “futuro”. Es decir, en Argentina por ejemplo, donde hasta el día de la fecha entendemos que no existe ISP alguno que realice la retención de datos de tráfico de forma voluntaria (ya que no existe obligación legal de realizarlo) dicha medida no tendría sentido, ya que las empresas responderían que no tienen ese tipo de datos.

Sin embargo, estamos convencidos que para aquellos delitos que se puedan dar de manera continuada o repetida en el tiempo, quizás pueda ser una medida útil

la guarda de datos de tráfico hacia el futuro, por un tiempo determinado y autorizado por la autoridad competente.

6.2.3. Orden de presentación

Esta medida tiene por destino ordenar a una persona (siempre dentro del territorio de donde emana esa orden) que comunique determinados datos informáticos que obren en su poder, o para que ordenen a un proveedor que ofrezca sus servicios en el territorio de dicha Parte que suministre información relativa a los abonados.

De acuerdo a lo desarrollado en los considerando del Convenio, se argumenta que la búsqueda de esta medida es evitar que los Estados apliquen sistemáticamente medidas coercitivas en relación con terceros, tales como el registro y la confiscación de datos. Una “orden de presentación” representa una medida flexible que las autoridades encargadas de hacer cumplir la ley pueden aplicar en muchos casos, especialmente en lugar de otras medidas más invasivas u onerosas.

La aplicación de este tipo de mecanismo procesal también será beneficiosa para los terceros encargados de la custodia de los datos, tales como los ISP, que en general están dispuestos a ayudar en forma voluntaria a las autoridades encargadas de hacer cumplir las leyes suministrando los datos que están bajo su control, pero que prefieren que exista una base jurídica adecuada para dicha asistencia, que los libere de toda responsabilidad tanto contractual como no contractual.

. La expresión “posea o que se encuentren bajo su control” se refiere a la posesión física de los datos en cuestión en el territorio de la Parte que imparta la orden y también a situaciones en las cuales la persona no tenga la posesión física de los datos que deben presentarse, pero que dicha persona pueda, no obstante, controlar libremente la presentación de los mismos desde dentro del territorio de la Parte que imparte la orden (por ejemplo, sujeto a los privilegios aplicables, una persona que recibe una orden de presentación de la información almacenada en su cuenta por medio de un servicio de almacenamiento en línea a distancia tiene la obligación de presentar esa información).

Por lo que respecta a las distintas modalidades de presentación de la información, podría establecerse la obligación de que los datos informáticos especificados o la información sobre los abonados se presente de la manera especificada en la orden. Ello podría incluir una referencia al período de tiempo en el cual se debe efectuar la revelación, o al formato, por ejemplo, que los datos o la información se presenten en "texto plano", en línea o impresa.

La expresión "datos relativos a los abonados" se define en el párrafo 3 del artículo del Convenio, por lo que remitimos nuevamente a lo ya desarrollado en la presente tesis en honor a la brevedad.

6.2.4. Registro y confiscación de datos informáticos almacenados

Como hemos adelantado, el derecho procesal penal de la mayoría de los países ya posee estas medidas de investigación pero de la forma tradicional, es decir, pensada para la evidencia física. Sin embargo, hemos desarrollado ya que los datos informáticos no son una cosa mueble o tangible, por lo que técnicamente dichas medidas no pueden aplicarse analógicamente.

En este contexto, la finalidad de la medida regulada por el artículo 19 del Convenio de Budapest busca establecer una facultad equivalente respecto de los datos almacenados.

Con respecto al registro para encontrar datos informáticos, en el nuevo entorno tecnológico, se siguen dando muchas de las características de un allanamiento tradicional. Por ejemplo, la obtención de los datos se lleva a cabo durante el allanamiento y está relacionada con datos que existen en ese momento. Las condiciones previas para la obtención de la autoridad legal para realizar un allanamiento siguen siendo las mismas. El grado de certeza requerido para obtener una autorización legal para efectuar un registro no es diferente, tanto si los datos están en forma tangible o en forma electrónica. Del mismo modo, las razones y el

registro guardan relación con datos que ya existen y que proporcionarán pruebas sobre un delito específico.

Sin embargo, por lo que respecta al registro en busca de datos informáticos, se necesitan nuevas disposiciones procesales a fin de garantizar la obtención de los datos informáticos de una manera que sea igualmente eficaz a la del registro y confiscación de un soporte de datos tangibles. Esto obedece a diferentes factores: en primer lugar, los datos se encuentran en forma intangible como, por ejemplo, en forma electromagnética. En segundo lugar, si bien los datos pueden ser leídos con el uso de equipos informáticos, no pueden ser confiscados y secuestrados de la misma manera que cuando se trata de un registro impreso. El medio físico en el que están almacenados los datos intangibles (por ejemplo, el disco duro de un ordenador o un cd) debe confiscarse o secuestrarse, o debe hacerse una copia de los datos, ya sea en forma tangible (por ejemplo, una copia impresa de los datos informáticos) o en forma intangible en un medio físico (por ejemplo, un disco rígido), antes de poder confiscar y secuestrar el medio tangible que contiene la copia. En las dos últimas situaciones, cuando se hacen copias de los datos, una copia de los datos queda en el sistema informático o en el dispositivo de almacenamiento.

En tercer lugar, debido a la manera en que están conectados los sistemas informáticos, los datos pueden no estar almacenados en el ordenador específico que se revisa, pero esos datos pueden ser de fácil acceso para dicho sistema. Podrían estar almacenados en un dispositivo conexo de almacenamiento de datos conectado directamente al ordenador o indirectamente a través de sistemas de comunicación, tales como Internet.

Esta situación también dispara diversos escenarios. Por un lado, si ese otro sistema se encuentra en el territorio, sería en principio necesario una ampliación de la orden[422] (o una nueva orden) que autorice el secuestro de datos en dicho servidor. Por otro lado, el escenario que el servicio donde está la información se encuentre fuera del territorio donde se autorizó la orden, donde estaríamos en presencia del

[422] El párrafo 2 permite a las autoridades encargadas de la investigación ampliar su registro o el acceso de un modo similar a otro sistema informático o parte del mismo si tienen motivos para creer que los datos buscados se hallan almacenados en ese otro sistema. No obstante, el otro sistema informático, o una parte del mismo, debe también estar situado “en su territorio”.

famoso acceso transfronterizo de datos, un tema increíblemente complejo que ya ha sido adecuadamente abordado por el maestro Marcos Salt en diversas oportunidades y al cuál haremos referencia al finalizar este capítulo, como uno de los grandes desafíos que aún no tiene una solución clara en el panorama jurídico.

En la medida sugerida por el Convenio de Budapest se hace referencia a la expresión "registren o tengan acceso de un modo similar". El uso de la palabra tradicional "registrar" indica que el Estado ejerce una facultad coercitiva, y que la facultad mencionada en este artículo es análoga al allanamiento tradicional. "Registrar" supone buscar, leer, inspeccionar o revisar datos. Incluye los conceptos de búsqueda de datos y de revisión (examen) de datos. Por otro lado, la palabra "acceso" tiene un sentido neutro, pero refleja más adecuadamente la terminología informática. Se utilizan ambos términos con el fin de vincular los conceptos tradicionales con la terminología moderna.

Sobre esta última distinción debemos recordar que las órdenes de autorización de la medida, pueden diferenciar en que permitan:

1. Exclusivamente el secuestro de dispositivos (ergo, no permitirían el acceso a los datos)
2. Exclusivamente el acceso (con copia por ejemplo) a los datos (por lo que no permitiría llevarse los equipos informáticos)
3. Autorice la copia de los datos, y en el caso de ser necesario (a criterio del personal que está realizando las operaciones informáticas o del fiscal a cargo), también existe autorización para secuestrar los dispositivos.

Actualmente, se está intentando evitar el secuestro de dispositivos, debido a la demora existente en los laboratorios forenses para realizar la extracción de la información (con una orden posterior). Adicionalmente, está avanzando notablemente el uso de cifrado de datos en los equipos personales, por lo que si se llega a tener la oportunidad de encontrar el equipo encendido (en el allanamiento) quizás esa sea la única oportunidad técnica de poder extraer información, toda vez que si dicho equipo es apagado y trasladado al laboratorio forense, posiblemente ya no pueda extraerse ningún tipo de información (consecuencia del cifrado, siempre que obviamente, no se tenga acceso a la clave que permitiría descifrar los datos).

Ingresando un poco más en la parte práctica de la medida, surgen tres variables críticas a considerar durante las actividades de identificación y preservación de evidencia digital: temporalidad, volumen y ubicuidad. La evidencia digital es capaz de permanecer en un dispositivo de almacenamiento por segundos o bien por años, puede tratarse de un solo bit o de millones de ellos y finalmente es susceptible de estar localizada en un único dispositivo de almacenamiento o distribuido por el mundo.

Existen diferentes aproximaciones para la recolección de adquisición de evidencia digital. Una de las modalidades más tradicionales es la incautación o secuestro del hardware u objeto de almacenamiento de los datos informáticos; otra de ellas es la adquisición completa de evidencia digital en el lugar del hecho; una variante de esta última es la adquisición selectiva de evidencia digital en el lugar del hecho; finalmente existen metodologías tipo "triage" a fin de realizar una identificación de evidencia digital relevante y una posterior recolección selectiva de fuentes de evidencia digital en el lugar del hecho a través de una capacitación mínima de las fuerzas de la ley[423].

Cada de una de estas variantes presenta beneficios y complicaciones, teniendo en cuenta los recursos necesarios para llevar a cabo tales medidas y las posibilidades de éxito de las mismas. Así la primera modalidad mencionada por ejemplo, no requiere de personal mayormente especializado en el área informática, ni de grandes recursos tecnológicos, al implicar simplemente la obtención física del objeto informático (hardware, Tablet, teléfono celular, etc.) y el traslado del mismo al personal especializado. Simplemente deberá el agente tener conocimiento y adecuarse a las guías y protocolos pertinentes al secuestro de un objeto y como preservarlo hasta tanto sea llevado al perito especialista que pueda analizarlo, asegurando la cadena de custodia. Por el contrario, las restantes modalidades implican un mayor conocimiento y especialización de quien lleva a cabo la medida, así como de recursos tecnológicos, toda vez que deberá ser personal entrenado quien tome, en el lugar del hecho una imagen forense, que podrá o no ser analizada luego en laboratorio. Estas opciones presentan como virtud el hecho de disminuir los

[423] CHALES, Juan Pablo; "Las técnicas de investigación penal a la luz del Convenio sobre ciberdelito y su aplicación en Argentina", Tesis de Maestría, 2018. Universidad Nacional de Cuyo.

riesgos de daños que implica el traslado del objeto, pero requiere de personal sumamente entrenado y de amplios recursos tecnológicos disponibles para las labores de campo. A su vez en el caso de

6.2.5. Obtención en tiempo real de datos informáticos (datos de tráfico / datos de contenido

Esta medida tiene por finalidad permitir a las autoridades avanzar hacia la obtención en tiempo real de datos sobre el tráfico y la interceptación en tiempo real de los datos sobre el contenido de comunicaciones específicas transmitidas por un sistema informático, ya sea de forma directa por las fuerzas de seguridad (en el caso que se tenga la capacidad técnica), o a través de la interceptación en tiempo real por parte de los proveedores de servicios.

Si bien las redes informáticas pueden tener una infraestructura fija independiente por cable, cada vez es más frecuente que funcionen como una red virtual que depende de conexiones efectuadas a través de las infraestructuras de telecomunicaciones, lo que permite crear redes informáticas, o enlaces de redes, de naturaleza global. La distinción entre las telecomunicaciones y las comunicaciones informáticas, y las especificidades de sus infraestructuras, son cada vez menos claras debido a la convergencia de las telecomunicaciones y las tecnologías de la información. Es por ello que la definición de “sistema informático” que se menciona en la medida sugerida, no restringe la manera en la cual pueden estar interconectados los dispositivos, o grupos de dispositivos.

Por consiguiente, los artículos 20 y 21 del Convenio de Budapest (recogida en tiempo real de datos de tráfico e interceptación de datos relativos al contenido) se refieren a comunicaciones específicas transmitidas por medio de un sistema informático, lo que podría incluir la transmisión de la comunicación a través de redes de telecomunicaciones antes de ser recibida por otro sistema informático.

Hacemos notar que (a diferencia por ejemplo de lo que ocurre con la tipificación penal ya vista en Argentina), las medidas sugeridas no establecen ninguna distinción entre un sistema de telecomunicaciones o un sistema informático

de carácter público o privado, ni entre la utilización de sistemas y servicios de comunicación ofrecidos al público o a grupos restringidos de usuarios o partes privadas, por lo que se entiende que no habría limitaciones en este sentido, aunque claro está, podría considerarse que la interceptación de datos en una red de telecomunicaciones "abierta" no estaría prohibida por ley (en Argentina por ejemplo), por lo que en consecuencia, podría ser discutible la necesidad de una autorización judicial para avanzar en dicha recolección.

Esta medida, a diferencia de las anteriores, rige la obtención de pruebas contenidas en comunicaciones que se están generando en el mismo momento que se produce la comunicación (es decir, "en tiempo real"), lo que implica una capacidad técnica y esfuerzo adicional para poder conseguir las mismas (y por eso, generalmente es necesario obtener cooperación por parte de los proveedores de servicios).

De esta forma, en vez de acudir a un secuestro físico de los datos, se realiza una grabación (es decir, una copia) de los datos que se están transmitiendo. La obtención de esas pruebas se lleva a cabo durante un determinado período de tiempo, por lo que (como veremos que sucede en España) se solicita autorización legal para permitir la obtención respecto de un acontecimiento futuro (es decir, la transmisión futura de datos).

De una comunicación electrónica es posible obtener dos tipos de datos: los datos sobre el tráfico y los datos sobre el contenido. De acuerdo con la definición del artículo 1.d del Convenio de Budapest se entiende por "datos sobre el tráfico" cualesquiera datos informáticos relativos a una comunicación por medio de un sistema informático, generados por un sistema informático como elemento de la cadena de comunicación, que indiquen el origen, destino, ruta, fecha, tamaño y duración de la comunicación o el tipo de servicio subyacente.

Sin embargo, en el Convenio no se define el término "datos sobre el contenido", pero éste se refiere al contenido informativo de la comunicación, es decir, el significado o la finalidad de la comunicación, o el mensaje o información transmitidos por la comunicación (excepto los datos sobre el tráfico).

En muchos Estados se establece una distinción entre la interceptación en tiempo real de datos sobre el contenido y la obtención en tiempo real de datos sobre el tráfico, tanto por lo que se refiere a los requisitos legales que deben cumplirse para que se autorice tal medida de investigación como a los delitos respecto de los cuales se puede emplear esta medida.

Si bien se reconoce que ambos tipos de datos llevan aparejados intereses relativos al respeto de la vida privada, muchos Estados consideran que la cuestión del respeto de la vida privada es más importante por lo que respecta a los datos sobre el contenido debido a la índole del contenido o del mensaje de la comunicación. Puede que se impongan mayores limitaciones con respecto a la obtención en tiempo real de los datos sobre el contenido que a los datos sobre el tráfico.

Para contribuir a reconocer la distinción que existe ambas situaciones se obtienen o registran datos, se refiere normativamente en los títulos de los artículos a la obtención de los datos sobre el tráfico como “obtención en tiempo real” y a la obtención de los datos sobre el contenido como “interceptación en tiempo real”. Dependiendo de cada país, la interceptación en tiempo real de datos sobre el contenido, en muchos casos la ley establece que la medida sólo es aplicable en relación con la investigación de delitos graves o de categorías de delitos graves. Estos delitos están definidos en el derecho interno de cada país como graves a tal efecto, y a menudo figuran en una lista de delitos aplicables o están incluidos en esta categoría porque se hace referencia a la sentencia máxima de prisión que es aplicable al delito.

En lo relativo a la obtención de datos sobre el tráfico, no está sujeto a ese tipo de limitación y, en principio, se aplica a todo delito penal contemplado en el Convenio. Sin embargo, el párrafo 3 del artículo 14 establece que cualquier Parte podrá reservarse el derecho a aplicar la medida exclusivamente a aquellos delitos o categorías de delitos especificados en la reserva, siempre que el ámbito de dichos delitos o categorías de delitos no sea más reducido que el de los delitos a los que se aplica la medida de interceptación de los datos sobre el contenido.

Como la interceptación de los datos sobre el contenido es una de las medidas de investigación más intrusivas de la vida privada, se requieren salvaguardias rigurosas para garantizar un equilibrio adecuado entre los intereses de la justicia y los derechos fundamentales de las personas. En el ámbito de la interceptación, el Convenio de Budapest no establece salvaguardias específicas aparte de limitar la autorización de la interceptación de los datos sobre el contenido a aquellas investigaciones que guarden relación con los delitos graves definidos en el derecho interno de cada país. Sin embargo, existe la libertad de aplicar condiciones y salvaguardias en las regulaciones internas, tales como: la supervisión judicial u otro tipo de supervisión independiente; la especificidad respecto de las comunicaciones o las personas a ser interceptadas, la necesidad, subsidiaridad y proporcionalidad (por ejemplo, los fundamentos jurídicos que justifiquen la adopción de la medida; la ineficacia de otras medidas menos intrusivas); una limitación respecto de la duración de la interceptación, el derecho a una compensación.

Muchas de estas salvaguardias reflejan lo dispuesto en el Convenio Europeo de Derechos Humanos y su jurisprudencia más importante en la materia, como pueden ser los casos Klass[424] , Kruslin[425] , Huvig[426] , Malone[427], Halford[428] y Lambert[429].

Tradicionalmente, la obtención de datos sobre el tráfico respecto de las telecomunicaciones (por ejemplo, las conversaciones telefónicas) ha sido una herramienta de investigación útil para determinar el origen o el destino (por ejemplo, los números de teléfono) y datos conexos (por ejemplo, la hora, la fecha y la duración) de diversos tipos de comunicaciones ilegales (por ejemplo, amenazas, hostigamientos, conspiración, tergiversaciones fraudulentas) y de comunicaciones que aportan pruebas de delitos pasados o futuros (por ejemplo, tráfico de drogas, asesinatos, delitos económicos, etc.).

[424] Sentencia del CEDH en el caso de Klass y otros contra Alemania, A28, 06/09/1978.
[425] Sentencia del CEDH en el caso de Kruslin contra Francia, 176-A, 24/04/1990.
[426] Sentencia del CEDH en el caso de Huvig contra Francia, 176-B, 24/04/1990.
[427] Sentencia del CEDH en el caso de Malone contra el Reino Unido, A82, 02/08/1984
[428] Sentencia del CEDH en el caso de Halford contra el Reino Unido, los informes de 1997 - III, 25/06/1997.
[429] Sentencia del CEDH en el caso de Lambert contra Francia, Informes, 1998 - V, 24/08/1998

Algo que destacamos de la explicación de esta medida (dentro de los considerandos y documentos explicativos, así como en discusiones previas) es que los datos sobre el tráfico que se desee obtener deben estar asociados con comunicaciones específicas. Es decir, se habla de "comunicaciones" específicas en plural, porque tal vez sea necesario obtener datos sobre el tráfico respecto de diversas comunicaciones con miras a identificar a las personas en su origen o destino (por ejemplo, en una casa donde varias personas utilizan las mismas instalaciones de telecomunicaciones, puede ser necesario establecer una correlación entre varias comunicaciones y las oportunidades que tuvieron esas personas para utilizar el sistema informático).

El Convenio no exige, ni autoriza la vigilancia y obtención generalizada o indiscriminada de grandes volúmenes de datos sobre el tráfico. No autoriza las "expediciones de pesca", en las que se abriga la esperanza de descubrir actividades delictivas, a diferencia de los casos concretos de delitos que se están investigando. La orden judicial o de otro tipo que autoriza la obtención de datos debe especificar las comunicaciones cuyos datos se desea obtener. Es decir, que deberán especificarse las comunicaciones respecto de las cuales se pueden obtener o registrar datos sobre el tráfico, teniendo así mayor protección sobre los datos de las personas y evitando, intromisiones innecesarias en su intimidad, aspecto que ya hemos desarrollado en el capítulo anterior.

Por último, diremos que al igual que ocurre con la interceptación en tiempo real de datos sobre el contenido, la obtención en tiempo real de datos sobre el tráfico sólo es eficaz si se lleva a cabo sin el conocimiento de las personas que están siendo investigadas. La interceptación es subrepticia y debe llevarse a cabo de manera tal que las partes que se comunican no se percatan de lo que está ocurriendo. Por consiguiente, los proveedores de servicios y sus empleados que tengan conocimiento de la interceptación deben cumplir con la obligación de guardar el secreto a fin de que el procedimiento pueda llevarse a cabo de manera eficaz.

6.3. Otras Medidas o técnicas especiales de investigación

Dedicaremos esta sección a realizar un repaso por una serie de otras medidas o técnicas especiales de investigación que, aunque han quedado fuera de las medidas sugeridas por el Convenio de Cibercrimen de Budapest, como veremos más adelante en este propio capítulo, ya se encuentran reguladas en algunos países (o en algunas provincias).

A modo preliminar y desde un punto de vista teórico, es posible realizar un agrupamiento de las medidas o técnicas de investigación tecnológica, identificando aquellas que tienen por objetivo la identificación del delincuente (por ejemplo, OSINT o Browser fingerprinting), sobre aquellas cuyo objetivo principal es la obtención de evidencia útil para la imputación del delito (descifrado compulsivo, acceso transfronterizo de datos, agente encubierto), aunque consideramos que lo cierto es que todas las medidas, podrían traer información útil para una u otra finalidad y en última instancia, su funcionalidad dependerá del caso concreto.

Sin más preámbulos, a continuación presentaremos una serie de medidas y técnicas de investigación tecnológicas, partiendo de la base que todas y cada una de ellas, puede ser merecedora de una tesis por si misma (de hecho, hay libros escritos sobre cada uno de estos temas). Por este motivo, y a la finalidad de esta tesis que es, reconocer su existencia, su problemática y sobre todo, los desafíos jurídicos que nos representan (y que en la mayoría de las casos aún no hay soluciones concretas a la vista), daremos un repaso lo más simple dentro de las posibilidades de cada temática.

6.3.1. OSINT (Open Source Intelligence)[430]

No podemos negar estar inmersos en un mundo repleto de información, donde cada parte de nuestra vida va quedando digitalizada y almacenada en distintos lugares cada vez más diversos y dispersos tales como gobiernos locales, provinciales, nacionales, extranjeros y empresas privadas. Ni hablar sobre la

[430] Basado en artículo “OSINT: Legalidad y protección de datos personales”, de Macedo Maximiliano y Temperini Marcelo, publicado en el libro “Protección de datos. Doctrina y jurisprudencia - Tomo 2”, dirigido por Pablo Palazzi,

explosión de uso de las distintas redes sociales y el paradigma de "compartirlo todo", configurado por defecto y con deficientes controles de privacidad.

A pesar de que las técnicas de OSINT provienen del ámbito militar, vale la pena aclarar que son cada vez más difundidas y utilizadas en diversos ámbitos como lo pueden ser el policial, periodístico, uso para áreas de fraude, uso por investigadores privados, uso empresarial entre otros. Estos usos y prácticas, muchas veces son realizados sin tener en cuenta el marco legal vigente, por lo cuál es una de las razones de manifestar la situación legal Argentina en torno a OSINT y explicitar su vinculación desde diferentes visiones de la problemática.

Al revisar la bibliografía específica sobre OSINT, ha sido posible observar diversas definiciones desde el ámbito militar y de defensa, en primera instancia tomaremos la definición del "Manual de la OTAN sobre OSINT"[431] donde dice textualmente "OSINT es información no clasificada, que ha sido descubierta de forma deliberada, discriminada, destilada y difundida a una audiencia selecta para abordar una pregunta específica de un tema", también citaremos la Departamento de Defensa de USA[432], "OSINT es inteligencia que es producida a partir de información disponible públicamente, se recopila, se explota y se difunde de manera oportuna a un público apropiado, con el propósito de abordar un requisito de inteligencia específico.". Ambas definiciones hacen mención a un esfuerzo por darle valor a la información obtenida y convertirla en inteligencia para necesidad de un objetivo específico.

Una primera referencia obligada desde el punto de vista normativo nos remite a la Ley Nº 25.520 sobre Inteligencia Nacional, en cuyo artículo 2 define qué se entenderá por inteligencia nacional "la actividad consistente en la obtención, reunión, sistematización y análisis de la información específica referida a los hechos, amenazas, riesgos y conflictos que afecten la seguridad exterior e interior de la Nación". En el inc. 3 del mismo artículo, se define a la Inteligencia Criminal como

[431] *"NATO Open Source Intelligence Handbook"* Noviembre 2001, Disponible en http://www.oss.net/dynamaster/file_archive/030201/ca5fb66734f540fbb4f8f6ef759b258c/NATO%20OSINT%20Handbook%20v1.2%20-%20Jan%202002.pdf

[432] United States Code, 2011 Edition. Title 50 - WAR AND NATIONAL DEFENSE, CHAPTER 15 - NATIONAL SECURITY, SUBCHAPTER I - COORDINATION FOR NATIONAL SECURITY, disponible en https://www.govinfo.gov/content/pkg/USCODE-2011-title50/html/USCODE-2011-title50-chap15-subchapI-sec403-5.htm

aquella "referida a las actividades criminales específicas que, por su naturaleza, magnitud, consecuencias previsibles, peligrosidad o modalidades, afecten la libertad, la vida, el patrimonio de los habitantes, sus derechos y garantías y las instituciones del sistema representativo, republicano y federal que establece la Constitución Nacional".

Si bien no es el objetivo de este trabajo, toda vez que su adecuado desarrollo implicaría dedicar el artículo completo a este subtema, debemos mínimamente decir que, en la actualidad Argentina, existe un contexto donde casi todas las fuerzas de seguridad, nacionales y provinciales, poseen sus propias estructuras dedicadas a la realización inteligencia (al menos de la criminal). Un informe[433] de una ONG Argentina aborda la historia normativa de los servicios de inteligencia de nuestro país, dando cuenta de los inaceptables grados de autonomía que poseen, y el riesgo que ello implica para los derechos de los ciudadanos y las instituciones democráticas.

En relación con el intento de establecer controles a la actividad de inteligencia, la Ley Nº 25.520 en su artículo 4 establece una serie de límites para todos los organismos, entre los que destacamos la prohibición del inc. 1 y 2. La primera de las prohibiciones, quizás la más importante para el tema, implica que ningún organismo podrá "*realizar tareas represivas, poseer facultades compulsivas, cumplir, por sí, funciones policiales ni de investigación criminal, salvo ante requerimiento específico realizado por autoridad judicial competente en el marco de una causa concreta sometida a su jurisdicción, o que se encuentre, para ello, autorizado por ley*".

Es decir, partimos de la base jurídica que, para poder llevar adelante tareas de inteligencia, el organismo deberá ser requerido por parte del poder judicial en una causa concreta sobre la cual tenga jurisdicción competente, o bien, existir ley especial que lo autorice. En general, las tareas de investigación con inteligencia criminal son muy comunes en el ámbito haciendo uso de la primera de las

[433] ADC, El (des)control democratico de los organismos de inteligencia en Argentina. Publicado en Enero 2015, Disponible en: https://adc.org.ar/wp-content/uploads/2019/06/004-el-descontrol-democratico-de-los-organismos-de-inteligencia-en-argentina-01-2015.pdf

excepciones, es decir, bajo requerimiento del fiscal (dentro del proceso penal acusatorio) y posterior autorización del juez.

A contrario sensu de la norma expuesta, podríamos inferir que toda tarea de inteligencia realizada por parte de personal de fuerzas de seguridad sin que exista requerimiento previo del poder judicial (excepto casos de existir ley especial que ordene) se encuentra prohibido. A nuestro entender, la misma conclusión también debería ser considerada para la realización de tareas de inteligencia por parte del ámbito privado (salvo excepciones).

La segunda y última prohibición que analizaremos implica que ningún organismo de inteligencia podrá "*obtener información, producir inteligencia o almacenar datos sobre personas, por el solo hecho de su raza, fe religiosa, acciones privadas, u opinión política, o de adhesión o pertenencia a organizaciones partidarias, sociales, sindicales, comunitarias, cooperativas, asistenciales, culturales o laborales, así como por la actividad lícita que desarrollen en cualquier esfera de acción*". Si bien aún no hemos abordado la práctica del OSINT desde la protección de datos, recomendamos al lector recordar esta prohibición en conexión con la categoría de datos personales sensibles de acuerdo con la Ley Nº 25.326.

6.3.1.1. La legalidad de la técnica desde la óptica de la Protección de Datos Personales

Si bien puede parecer que el OSINT no siempre está dirigido a la obtención de datos personales de forma directa, lo cierto es que es imposible generar un informe de OSINT sin considerar que existen datos personales. El concepto amplio de nuestra normativa, incluyendo a cualquier tipo de información que haga a una persona determinada o determinable, termina respondiendo a esa pregunta.

Por poner un ejemplo, la clásica recolección de información desde una cuenta de una red social que contiene información de forma "pública" (que ya veremos que no es lo mismo que entender que es una fuente de acceso público irrestricto), implica recolectar información sobre amistades, fotos, comentarios de personas

relacionadas, en definitiva, todo lo que podría obtenerse de dicha fuente, son datos personales sin lugar a duda.

Por otro lado, las definiciones que repasamos también nos ayudan a responder otra posible pregunta de algún investigador, acerca de considerar que sus informes de OSINT sean considerados una "base de datos". La claridad normativa no deja tampoco lugar a dudas, entendiendo que todo informe es un conjunto organizado de datos personales, electrónicos o no, y cualquiera fuere la modalidad de su formación[434].

A modo de complemento, relacionado a lo señalado anteriormente sobre la posibilidad de realización de OSINT por parte de personas privadas, el artículo 4 de la Ley Nº 25.326, inc. 2, establece que "*La recolección de datos no puede hacerse por medios desleales, fraudulentos o en forma contraria a las disposiciones de la presente ley*". Podríamos preguntarnos, la recolección de información que se está realizando por parte de un privado ¿es leal? ¿la persona investigada, sabe que se están recolectando y tratando sus datos personales? ¿se le informa de alguna manera a fin de que pueda ejercer los derechos que le corresponden?

Estas preguntas nos presentan la puerta de entrada para analizar si existe el consentimiento, o en su caso, si se necesita el consentimiento para realizar dicho tratamiento. De acuerdo con el art. 5[435], el principio marca que el tratamiento es

---

[434] Ley Nº 25.326; Art. 2: *Archivo, registro, base o banco de datos: Indistintamente, designan al conjunto organizado de datos personales que sean objeto de tratamiento o procesamiento, electrónico o no, cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso.*

[435] Ley Nº 25.326; Art. 5: *1. El tratamiento de datos personales es ilícito cuando el titular no hubiere prestado su consentimiento libre, expreso e informado, el que deberá constar por escrito, o por otro medio que permita se le equipare, de acuerdo a las circunstancias.*
El referido consentimiento prestado con otras declaraciones, deberá figurar en forma expresa y destacada, previa notificación al requerido de datos, de la información descrita en el artículo 6° de la presente ley.
2. No será necesario el consentimiento cuando:
a) Los datos se obtengan de fuentes de acceso público irrestricto;
b) Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal;
c) Se trate de listados cuyos datos se limiten a nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio;
d) Deriven de una relación contractual, científica o profesional del titular de los datos, y resulten necesarios para su desarrollo o cumplimiento;
e) Se trate de las operaciones que realicen las entidades financieras y de las informaciones que reciban de sus clientes conforme las disposiciones del artículo 39 de la Ley 21.526.

ilícito si el titular no presta consentimiento libre, expreso e informado, cuestión que descartamos que exista en alguna investigación (de OSINT o de otro tipo).

El primero de los incisos marca quizás uno de los conceptos más debatidos en esta temática, al mencionar que dicho consentimiento no será necesario si las fuentes son de "acceso público irrestricto". ¿Cuáles son las fuentes de acceso público irrestricto? ¿Son las redes sociales este tipo de fuentes?

En el Dictamen 3/2004[436], con un planteo sobre el alcance de dicho concepto, se manifestó: "*La Ley Nº 25.326 define a una base como "pública" no por la posibilidad de acceso del público a la información contenida en ella, sino por su titularidad por parte de un organismo público. De esta manera, como ya ha tenido oportunidad de señalar este Órgano de Control, la información registrada en una base de datos pública puede ser clasificada en tres niveles de intensidad de la publicidad de los datos que registra: a) Información confidencial: Es aquella afectada por un secreto o confidencialidad legal Ej. Secreto profesional, bancario, fiscal, datos sensibles, etc.), derechos de terceros (ej. intimidad), etc. b) Información de acceso público: Es la información en poder de la Administración que no está sujeta a confidencialidad ni tampoco está destinada a ser difundida irrestrictamente al público, y que generalmente su acceso por parte de terceros resulta condicionado al cumplimiento de ciertos requisitos. c) Información de acceso público irrestricto: Es aquella información destinada a ser difundida al público en general y de libre intercambio entre los organismos del Estado*."

En esta categorización realizada por la autoridad de aplicación, queda claro que esta primera excepción a la necesidad del consentimiento fue pensada para aquella información emitida por parte de un organismo público, y además, destinada a ser difundida al público en general. Entre los ejemplos que podríamos citar, se encuentra la publicación de sentencias, normas, boletín oficial, entre otras fuentes de información pública de acceso público irrestricto.

Adicionalmente a este Dictamen, la Ley 1845 (2005) de Protección de Datos Personales de Ciudad Autónoma de Buenos Aires, en su art. 3, establece

[436] Dirección Nacional de Protección de Datos Personales; Dictámen DNPDP Nº 3/04, Disponible en: https://www.argentina.gob.ar/sites/default/files/d2004_003.pdf

expresamente entre sus definiciones que se entenderá por Fuentes de acceso público irrestricto, indicando que "exclusivamente, se entienden por tales a los boletines, diarios o repertorios oficiales, los medios de comunicación escritos, las guías telefónicas en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección o cualquier otro dato que indique de su pertenencia al grupo".

En relación con la potencial afectación de la privacidad de los titulares de los datos incluidos en estas fuentes de acceso público irrestricto, en el año 2003, el Grupo de Trabajo del art. 29[437] (UE) observó que el artículo 5 de la Ley Nº 25.326 permite el tratamiento de datos personales sin el consentimiento del titular de los datos si los datos se obtienen de fuentes de acceso público irrestricto. En el informe, el Grupo de Trabajo "*considera que es necesario establecer normas que garanticen que los datos incluidos en una fuente de acceso público irrestricto sean de tal naturaleza que no sea probable que su tratamiento sin el consentimiento del titular pueda suponer un riesgo para los derechos fundamentales y las libertades del individuo y, concretamente, para su derecho a la intimidad. Se sobreentiende que, incluso en el caso de que se incluyan datos personales en una fuente de acceso público irrestricto, es aplicable todo lo dispuesto en la legislación argentina sobre protección de datos.*"

Repasado el concepto de fuentes de "acceso público irrestricto", queda claro que las redes sociales distan de serlo, por lo que mal podría utilizarse dicho argumento para avanzar sobre la recolección de dichos datos en este tipo de fuentes.

La segunda de las excepciones enumeradas en el art. 5, establece que no será necesario el consentimiento cuando "*Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal*", que sería el caso de interés para el tema de la presente tesis. Esta excepción sería plenamente aplicable para el caso de fuerzas de seguridad cuyas tareas de investigación en

[437] EUROPEAN DATA PROTECTION BOARD, Legado: Grupo de Trabajo del art. 29; Disponible en: https://edpb.europa.eu/our-work-tools/article-29-working-party_es

OSINT están fundadas en requerimientos judiciales, de acuerdo con lo ya desarrollado anteriormente sobre la Ley de Inteligencia Argentina.

Por otro lado, esta excepción confirma a su vez, la ilegitimidad de todo tratamiento de datos personales realizado por personal que estuviera dentro de las funciones propias del Estado. Es decir, se confirma la necesidad de consentimiento por parte de los investigados para el caso de querer practicar OSINT por parte de investigadores privados, o bien, de investigadores de fuerzas de seguridad que no hayan recibido autorización o requerimiento judicial.

La tercera excepción, del inc. C, indica que no será necesario el consentimiento cuando "*se trate de listados cuyos datos se limiten a nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio*". Si bien aquí podrían quedar habilitados los investigadores privados, lo cierto es que raramente alguna investigación de OSINT se limita solamente a estos datos personales básicos del padrón electoral, sino que generalmente incorpora un universo de datos personales mucho más amplio (fotos, comentarios, correos electrónicos, número de teléfono, y un largo etc.).

6.3.1.2. OSINT y su función en la prevención policial del delito

En el contexto de pandemia mundial, en Mayo de 2020, el Ministerio de Seguridad de la Nación Argentina, a través de la Resolución 144/2020[438], presentó el "Protocolo General para la Prevención Policial del Delito con Uso de Fuentes Digitales Abiertas", del cual procederemos abordar algunos aspectos generales más relacionados con el tema que nos convoca.

Lo primero que nos interesa destacar, es el concepto que se expresa en su art. 2[439], donde observamos que el concepto ensayado vuelve a aportar a la confusión

[438] MINISTERIO DE SEGURIDAD DE LA REPÚBLICA ARGENTINA, Resolución 144/2020: "Protocolo General para la prevención policial del delito con uso de fuentes digitales abiertas"; Disponible en: https://www.boletinoficial.gob.ar/detalleAviso/primera/230060/20200602

[439] Protocolo General para la Prevención Policial del Delito con Uso de Fuentes Digitales Abiertas; Art. 2: "*Se entiende por "fuentes digitales abiertas" a los medios y plataformas de información y comunicación digital de carácter público, no sensible y sin clasificación de seguridad, cuyo acceso no implique una vulneración al derecho a la intimidad de las personas, conforme lo normado en la Ley de Protección de Datos Personales N° 25.326 y sus normas reglamentarias*"

entre datos abiertos y los de "carácter público" como describe su definición. Por otro lado y a diferencia de la definición del Convenio de Budapest, aquí se introducen una serie de requisitos extras para que puedan operar como fuente abierta de acuerdo con el Protocolo, entre los que destacamos la no vulneración al derecho a la intimidad de las personas y el cumplimiento a lo normado en la Ley de Protección de Datos Personales, aspecto que nos remite a las reflexiones ya analizadas. Adicionalmente, destacamos que incluye que quedarían exceptuados de ser recolectados los datos "sensibles", que en los términos del concepto definido por la Ley Nº 25.326, tendría coherencia con una de las prohibiciones que hemos repasado en la Ley de Inteligencia, en su art. 4 inc. 2. Incluso, entre las prohibiciones incluidas en el mismo Protocolo, en el art. 8 inc. 1, se reiteran varias de estas categorías de datos.

Avanzando con el protocolo, entre los delitos que se podrían prevenir estipula en el art. 3 qué fuerzas federales deben atender "*la comercialización, distribución y transporte de medicamentos apócrifos y de insumos sanitarios críticos; la venta de presuntos medicamentos comercializados bajo nomenclaturas y referencias al COVID-19 o sus derivaciones nominales, sin aprobación ni certificación de la autoridad competente; y a los ataques informáticos a infraestructura crítica —especialmente a hospitales y a centros de salud*".

Si bien la vigencia del protocolo estaría determinada a la duración de la situación de emergencia pública en materia sanitaria establecida por Ley Nº 27.541 (y sus posteriores decretos que amplían su plazo), en el segundo párrafo del art. 3, se amplía el alcance a partir de la siguiente fórmula: "*Asimismo, en tanto se advierta que resulten sensibles al desarrollo de la emergencia pública en materia sanitaria […], podrán definirse como objeto de las tareas de prevención policial con uso de fuentes digitales abiertas, posibles conductas delictivas cuyo medio comisivo principal o accesorio incluya la utilización de sistemas informáticos con el fin de realizar acciones tipificadas penalmente como la trata de personas; el tráfico de estupefacientes; el lavado de dinero y terrorismo; conductas que puedan comportar situaciones de acoso y/o violencia por motivos de género, amenaza y/o extorsión de dar publicidad a imágenes no destinadas a la publicación; y delitos relacionados con*

el grooming y la producción, financiación, ofrecimiento, comercio, publicación, facilitación, divulgación o distribución de imágenes de abuso sexual de niñas, niños y adolescentes".

Es decir, si bien inicialmente el objetivo era la utilización de la prevención policial del delito para fines relacionados a la emergencia sanitaria, se ha decidido incorporar algunos de los delitos que más suelen dejar "rastros" en internet. Abordaremos mayores detalles de dicha normativa al analizar el caso puntual de la regulación a nivel federal de Argentina.

6.3.2. Agente encubierto informático o digital

Esta medida consiste en la utilización a través de medios electrónicos, de una identidad supuesta, para poder entrar en el ámbito de confianza del sujeto investigado, y desde la cuál se busca obtener información de interés para una causa previamente determinada[440].

La justificación de este tipo de medidas, en muchos casos tiene relación con el nivel de resguardos técnicos que tiene el ciberdelincuente para ocultar su identidad y ubicación, por lo que esta figura puede volverse de importancia para poder establecer información de utilidad relacionada a su identificación, o bien, que permita acreditar la comisión de uno o más delitos por parte del sujeto investigado.

Más allá de los aspectos técnicos sobre el ocultamiento de la identidad, el agente encargado de dicha tarea generalmente utiliza técnicas de "ingeniería social"[441] para lograr engañar a la persona investigada, y lograr obtener la información que se necesita para la investigación.

Para comenzar con la fundamentación, nos parece acertado citar el análisis realizado por María Victoria Rodríguez Caro, Licenciada en Derecho y en

[440] TEMPERINI, Marcelo y MACEDO, Maximiliano, "Nuevas herramientas para la investigación penal: El agente encubierto digital", Cibercrimen. Aspectos de derecho penal y procesal penal. Cooperación internacional. Recolección de evidencia digital. Responsabilidad de los proveedores de servicios de Internet. Editora: Daniela Dupuy. Editorial: BdeF, 2017.
[441] ANDERSON, Ross. "Security engineering: a guide to building dependable distributed systems". Editorial Wiley, ISBN 978-0-470-06852-6.

Criminología; Máster en Sistema penal, Criminalidad y Políticas de Seguridad, Abogada y Fiscal Sustituta. En un artículo de doctrina[442] publicado por esta autora, se realiza un especial comentario en lo que se ha dado en llamar ciberdelincuencia, cuya importancia ascendente motiva la necesidad de reformas o adaptaciones en relación a las herramientas de investigación. En palabras de esta autora, "*Internet constituye un nuevo espacio en el que se desarrolla la actividad delictiva más diversa, y la figura del agente encubierto se muestra como un medio eficaz para el descubrimiento y la persecución de quienes se aprovechan de la red para sus propósitos*".

Sostiene Rodriguez Caro que los factores que ya se analizaron en cuanto al desarrollo de la ciberdelincuencia, especialmente el anonimato, la falta de contacto directo delincuente víctima y la prosperabilidad del engaño, son los que "*hacen adecuada la investigación encubierta para el descubrimiento de los responsables de este tipo de delitos, especialmente graves por la vulnerabilidad de los destinatarios del ataque*". Se hace también un interesante análisis acerca del concepto de organización en la red, a fin de analizar si sería aplicable la figura considerando que estos delitos en internet, podrían llegar a ser considerados como crimen organizado. En este sentido, Rodriguez Caro trabaja que el concepto de organización en la red también presenta perfiles propios, lo que se refleja en la propia posición de la jurisprudencia (española).

Conforme a la dictado en una Sentencia del Tribunal Supremo, "*tendrán la consideración de grupos organizados cualesquiera aquellos lugares de encuentro que son utilizados en Internet para la interrelación de diversas personas en torno a un tema común y con la finalidad, en muchos casos, de intercambiar material multimedia referido a ese tema, cómo serían los chats, comunidades virtuales, redes sociales, blogs, etc.*"[443]

Por el contrario, otra sentencia del mismo tribunal[444] opta por un concepto más restrictivo, para que pudiera hablarse de organización delictiva, sería necesaria una

[442] RODRÍGUEZ CARO, María Victoria. "La infiltración policial: en el límite del Estado de Derecho. El inminente agente encubierto informático"; Editorial Academica Espanola (8 Junio 2015)
[443] STS 1444/04, de 10 de diciembre
[444] STS 913/2006, de 20 de septiembre

estructura más compleja que la existente en los referidos lugares de encuentro de Internet. Esta autora realiza aquí un razonamiento en cuanto al nacimiento de la figura del agente encubierto para la investigación del narcotráfico, actividad esencialmente organizada, que dota de una especial gravedad y trascendencia socio-económica al delito de tráfico de drogas, especialmente nocivo cuando penetra en las instituciones del mismo Estado. Y lo que para este caso se preveía como natural, para el resto de los delitos se convierte en un estándar de proporcionalidad.

Es decir, de acuerdo a estos criterios es posible la implementación de la investigación encubierta cuando, aun tratándose de la investigación de delitos menos graves se trate de investigaciones que afecten a actividades propias de la delincuencia organizada. La razón de ser radica, de un lado en la especial gravedad de los delitos cometidos por las organizaciones criminales debido a la mayor facilidad para la perpetración por los mecanismos y medios empleados, el incremento de la impunidad que proporciona a los integrantes de la organización, así como de los potenciales efectos del delito; junto a ello, se justifica la necesidad de emplear medios de investigación nuevos para formas nuevas de delincuencia, allí donde fracasan los métodos tradicionales.

En relación a este desarrollo, nos parece oportuno aquí destacar unas líneas sobre la jurisprudencia ya vista de nuestra CSJN, en el caso "Fiscal c/ Fernandez"[445] donde se afirmó que "*el hecho comprobado de que ciertos delitos de gravedad se preparan e incluso ejecutan en la esfera de intimidad de los involucrados en ellos, como sucede particularmente con el tráfico de estupefacientes, impone reconocer que esos delitos sólo son susceptibles de ser descubiertos y probados si los órganos encargados de la prevención logran ser admitidos en el círculo de intimidad en el que ellos tienen lugar*". Siguiendo esta línea de razonamientos, la CSJN reconoce que la figura del agente encubierto, se encuentra fundamentada en que estamos ante la presencia de delitos graves y cuya ejecución se realiza dentro de un círculo de intimidad, ambos requisitos cumplidos cuando nos enfrentamos a la investigación de delitos cuyo bien jurídico afectado es la integridad de un menor, y donde se utiliza la tecnología como medio de comisión, dotando de complejidad a la detección e

[445] CSJN, "Fiscal c/Fernández, Víctor Hugo", sentencia del 11/12/1990, Fallos 313:1305

identificación de los autores, así como en una adecuada recolección de la evidencia digital.

En este mismo sentido, el autor Hugo Vaninetti[446] sostiene que la figura del agente encubierto para la investigación de los delitos relacionados con el material de abuso sexual infantil en internet debe ser legislada y de manera muy estricta. Este autor trabaja un tema interesante en cuanto a la interpretación de la figura del agente encubierto, expresando que las infiltraciones sencillas, que tan sólo afloran la previamente exteriorizada voluntad delictiva de quien ofrece el objeto prohibido (por ejemplo en el caso de abuso sexual infantil), no se pueden confundir con la provocación delictiva, ni precisan de más exteriorizaciones oficiales de la "simulación" del agente encubierto que las justifique ya que están dadas en el marco de la previa autorización judicial dando cuenta inmediata al Juez de todo hecho relevante en la investigación.

Se entiende que esta cuestión es sin dudas debatible y que demandará claras disputas doctrinarias que son necesarias abordar, y que lamentablemente (como nos sucede con otros tantos temas de interés) exceden el objeto de esta tesis. Entendemos que ante el avance de la delincuencia informática se hace necesario plantear y crear nuevas formas de concepción en la investigación de las mismas, sin apartarse del marco referencial prioritario de los derechos y garantías constitucionales. Vaninetti concluye afirmando que "*la restricción clásica de que deben existir previos indicios serios judicialmente ponderados y autorizados para permitir operaciones de infiltración no siempre ha de ocurrir tajantemente en Internet, puesto que la volatilidad de la información y lo variable de la misma hacen que la tarea del agente encubierto designado debería poder efectuarse igualmente mediante monitoreos en la red (las llamadas prospecciones), de lo contrario se perdería un precioso tiempo para detectar tales prácticas ilícitas*"[447].

La importancia de este desarrollo sobre la necesariedad de la medida, tiene como corolario afirmar que todos estos aspectos que son determinantes de la

[446] VANINETTI, Hugo "Agente encubierto y la pornografía infantil en internet", publicado en LA LEY, DJ 02/11/2011, Cita Online: AR/DOC/2722/2011
[447] VANINETTI, Hugo "Agente encubierto y la pornografía infantil en internet", publicado en LA LEY, DJ 02/11/2011, Cita Online: AR/DOC/2722/2011

gravedad de las conductas y justifican el empleo de un agente de seguridad infiltrado, concurren en el caso de los delitos cometidos a través de Internet (incremento de la facilidad de perpetración, de la impunidad y de los efectos), en especial la necesidad de emplear métodos nuevos allí donde los tradicionales no alcanzan (máxime cuando se trata de delitos conectados con casos de abuso sexual infantil).

6.3.2.1. La diferencia entre Agente encubierto digital y el Ciberpatrullaje

El ciberpatrullaje consiste en el acceso, análisis y procesamiento masivo de información disponible en internet, buscando detectar comportamientos criminales en línea que, en caso de reunirse algunos indicios o elementos, podría dar lugar al inicio de una investigación penal concreta. De todas las medidas listadas, esta es la única que no refiere a la investigación de un delito concreto, sino que es una actividad de prevención que suele ser cada vez más realizada por distintas fuerzas alrededor del mundo[448].

La diferencia entre el ciberpatrullaje y el agente encubierto digital (otras de las medidas listadas), es que en este último la fuerza de seguridad que oculta su identidad, lo hace con un objetivo concreto -la obtención de información útil para una investigación ya en curso-. En cambio, en el ciberpatrullaje es una etapa previa, donde ni siquiera es necesario ocultar la identidad del agente de seguridad, toda vez que estamos ante casos cuya exposición pública (sin límites de privacidad) permite un acceso irrestricto a la información por parte de cualquier usuario.

Se diferencia también de la inteligencia sobre fuentes abiertas, que allí también suele utilizarse para casos ya en curso (si bien puede ser etapa preliminar) donde ya existió una “notitia criminis” sobre el hecho que se está intentando averiguar.

De acuerdo a las conclusiones de la II jornada sobre el marco jurídico de actuación del agente encubierto[449], esta actuación policial inicial en la web que puede realizarse sin necesidad de una previa autorización judicial del agente

[448] CLARIN, “Se relanzó la Policía Federal con su nueva función de "ciberpatrullaje", Url: https://www.clarin.com/policiales/relanzo-policia-federal-nueva-funcion-ciberpatrullaje_0_B1KKunQ0x.html
[449] Ministerio de Justicia de España, Madrid, 29 de mayo de 2015.

encubierto virtual o informático. Allí consideraron que estos "*rastreos policiales que se efectúan en espacios de libre acceso como las redes P2P o en determinados ámbitos de las redes sociales o en general en foros abiertos de internet. Es una técnica policial perfectamente válida y en la que no son exigibles requisitos especiales.*"

El acceso a internet y a los rastros que el delincuente deja en él, no afecta a derechos fundamentales, pues ni es privado ni íntimo lo que se deja allí, ni se trata de una telecomunicación formalmente protegida cuyo secreto deba guardarse, ni son datos protegidos automatizadamente los que se realizan al colgar en internet ofertas, más o menos camufladas de objetos de circulación delictiva.

En los delitos en los que se expone el contenido ilícito (ej. venta de droga, reclutamiento de terroristas, intercambio de material de abuso sexual infantil, etc) utilizando internet como medio de difusión hay un claro propósito previo del investigado a delinquir, exteriorizado al dirigirse a un círculo más o menos amplio y generalmente anónimo de presuntos destinatarios desconocidos, de cuya actuación precisa para materializarse y consumarse la acción. La oferta supone la cesión anónima a todos sus presuntos aceptantes de los datos que se expongan al hacerlo, que obviamente, habilitan que los cuerpos de seguridad puedan avanzar en su investigación.

Es de frecuente utilización en las investigaciones policiales en la red el uso procedimientos mecánicos o automatizados[450], es decir, utilización de sistemas de rastreo que debidamente programados y a partir de voces o de conceptos realizan búsquedas en foros abiertos. Se trata también de una concreta ejecución de las funciones de prevención del delito a que se refiere el artículo 11 de la Ley de Fuerzas y Cuerpos de Seguridad o de las que corresponden a la policía judicial a tenor de lo establecido en el artículo 282 de la LECrim[4].

En relación con el *ciberpatrullaje* o rastreo policial ha tenido oportunidad de pronunciarse en múltiples ocasiones el Tribunal Supremo Español, como por

[450] El programa denominado "Quijote" creado por alumnos de la Cátedra Amaranto de Seguridad Digital e Internet del Futuro. La herramienta está diseñada para la localización de los usuarios que comparten material de abuso sexual infantil. . El "Quijote" centra su búsqueda en redes Peer to Peer (P2P) y en archivos multimedia, es decir, fotografías o videos.

ejemplo en la STS 236/2008, de 9 de mayo, señalaba que "*los rastreos que realiza el equipo de delitos telemáticos de la Guardia Civil en internet tienen por objeto desenmascarar la identidad críptica de los IPS (Internet protocols) que habían accedido a los "hash" que contenían material de abuso sexula infantil. El acceso a dicha información, calificada de ilegítima o irregular, puede efectuar cualquier usuario. No se precisa de autorización judicial para conseguir lo que es público y el propio usuario de la red es quien lo ha introducido en la misma*".

6.3.3. Registro remoto sobre equipos informáticos

6.3.3.1. Registro remoto en allanamientos tradicionales

Para comenzar a desarrollar este complejo tema de los registros remotos o a distancia, considero la necesidad de agregar este pequeño subtítulo a fines de abordar una confusión que advierto cada vez más presente en relación a lo que implica la medida del registro remoto.

Entendemos que se hace importante diferenciar la habilitación de realizar registro remoto de datos (en el marco de un allanamiento tradicional) de un registro remoto que pretende, de forma subrepticia (y sin involucrar un allanamiento tradicional) acceder a datos de interés para la investigación.

La primera de las opciones, es algo mucho más sencillo técnicamente e implica que, en el marco de un allanamiento tradicional de un domicilio, previa autorización del juez competente, los expertos en forensia digital puedan realizar la extracción de datos de un equipo que se encuentra encendido y desbloqueado, a partir de una conexión remota, procedimientos que por ejemplo ya se han realizado en la Provincia de Córdoba[451] (Argentina).

Técnicamente, se provee al personal policial o investigador a cargo de pendrives que contienen software portable (es decir, que no necesita ser instalado), con copia doble para eliminar la probabilidad de que ocurra un error de lectura. El

[451] DIARIO LA IMPRENTA; "Novedoso: El Ministerio Público Fiscal de Córdoba realiza con éxito allanamientos en remoto", Disponible en: https://diariolaimprenta.com.ar/novedoso-el-ministerio-publico-fiscal-de-cordoba-realiza-con-exito-allanamientos-en-remoto/

pendrive es montado en el dispositivo identificado como evidencia digital y, desde una computadora propiedad del poder judicial, un técnico informático (autorizado previamente por el juez) accede, de manera remota, al contenido existente en la evidencia digital, verificando y extrayendo los elementos que resulten de interés para la causa.

La utilidad de ese tipo de registro remoto, tiene que ver con evitar el traslado de personal capacitado, que muchas veces precisa estar dentro del laboratorio forense realizando otras tareas técnicas. Es importante tener en consideración que esta técnica tiene sentido únicamente ante la autorización pertinente de la requisa o registro de datos. Recordemos siempre la diferencia entre lo que implica el secuestro de los dispositivos que contienen datos por sobre la autorización al acceso y secuestro (copia en realidad) de los datos informáticos que puedan ser de interés.

La posibilidad tecnológica actual (considerando que se posee una buena conexión a internet), permite o habilita que las mismas tareas que podría realizar un especialista sentado delante del equipo, también pueda ser realizada a distancia, de forma remota, siempre contando con algún tipo de asistencia básica en el lugar de los hechos (puntualmente, que permita y habilite la recolección remota).

Entendemos que esta posibilidad de registro remoto, es algo que será cada vez más común en los procedimientos de las fuerzas de seguridad y es algo que, si bien consideramos que debe estar expresamente autorizado por el juez competente, no tiene las mismas implicancias (y riesgos jurídicos) que el otro tipo de registro o allanamiento remoto.

Como veremos a continuación, la segunda opción es probablemente la más polémica, por un lado por la novedad investigativa que plantea y por otro, por la grave afectación a la intimidad que representa para la persona investigada. Sobre esta segunda medida, abordaremos a continuación el resto del desarrollo.

6.3.3.2. Registro remoto subrepticio como alternativa al allanamiento

Esta medida consiste en la utilización de datos de identificación (credenciales), así como la instalación de software especializado, que permita de forma remota y telemática, el examen a distancia y sin conocimiento de su titular del contenido de un sistema informático.

De todas las medidas y técnicas de investigación tecnológica, probablemente esta sea la más agresiva y peligrosa, por lo que en muchos países[452], su regulación aún se encuentra en debate.

Comenzaremos advirtiendo que la ejecución de esta medida implica implica la instalación de un virus (malware) en el dispositivo electrónico a investigar, lo cual implica recurrir a las mismas herramientas o similares que las que utilizan los ciberdelincuentes, lo que plantea desde el comienza una cuestión acerca de que las herramientas estatales deben cumplir con una serie de requisitos adicionales que las diferencian de los cibercriminales para crear botnets o sustraer dato privados.

A diferencia de lo que puede ocurrir en el ámbito de la ciberdelincuencia y la explotación de vulnerabilidades, donde “todo vale” para poder acceder ilegítimamente a los servicios de la víctima, la demanda de herramientas de interceptación especializada por parte del Estado, implican la exigencia de un funcionamiento que debe superar el estándar meramente probabilístico de los típicos exploit ilegales. “En efecto, el malware estatal debe tener una alta probabilidad de comprometer exitosamente el equipo de su objetivo sin alterarlo y sin perturbar el funcionamiento de ese equipo ni de ningún otro. Además, debe permitir que quienes lo operan confirmen rápidamente si ha tenido éxito o no, que se lo controle durante el tiempo que dure la intervención legalmente autorizada y que pueda ser eliminado sin dejar rastros una vez que aquella concluya”[453].

---

[452] Diario Judicial, “¿Se viene el "troyano judicial"?”, Url: http://www.diariojudicial.com/nota/80621

[453] BLANCO, Hernán, Tecnología Informática e investigación criminal, Ciudad Autónoma de Buenos Aires,La Ley, 2020, pág. 103. Con cita de Bellovin, Steven M. – Blaze, Matt – Clark, Sandy – Landau, Susan, “Going bright: Wiretapping without weakening communications infraestrcuture”, en IEEE Security & Privacy, vol. 11, Nro. 1, 2013, Págs. 62/72.

Un exploit es un programa o código que "explota" una vulnerabilidad (defecto o debilidad de un sistema o de parte de él) para aprovecharla. El exploit no es un código malicioso (malware) en sí mismo, habitualmente se lo utiliza como un componente dentro del malware. Los malware generalmente utilizan los exploit como "llaves" para acceder a un sistema vulnerable. Existen diversos tipos de exploit dependiendo las vulnerabilidades. Las vulnerabilidades más valiosas son las Zero Day (día cero) por ser desconocidas para el fabricante del programa y no haber sido mitigadas por un parche[454].

En lo relativo al registro remoto propiamente dicho, Hernán Blanco[455] estaca que se divide en cuatro:

1) Envío (delivery): envío del exploit por internet (Ej.: mensaje de correo o mensaje SMS) o en forma física,

2) Intrusión (exploitation): aprovechamiento de la vulnerabilidad a través del exploit para superar defensa e instalar el programa malicioso,

3) Ejecución y

4) Reporte (reporting)

Siguiendo la letra del artículo 588 septies "a" de la Ley de Enjuiciamiento Española que ya hemos pasado, en su punto 2 "b" establece que el juez deberá especificar: "*El alcance de la misma, la forma en la que se procederá al acceso y aprehensión de los datos o archivos informáticos relevantes para la causa y el software mediante el que se ejecutará el control de la información*."

El penalista y autor Diego Stratiotis sostiene que "*es muy importante que se determine el alcance de la misma y principalmente que se determine qué se busca en el dispositivo del sospechoso, sin embargo ¿qué nivel de especificación se lo*

[454] SEGU-INFO; Url: https://www.segu-info.com.ar/malware/exploit

[455] BLANCO, Hernán, Tecnología Informática e investigación criminal, Ciudad Autónoma de Buenos Aires,La Ley, 2020, pág. 103. Con cita de Bellovin, Steven M. – Blaze, Matt – Clark, Sandy – Landau, Susan, "Going bright: Wiretapping without weakening communications infraestrcuture", en IEEE Security & Privacy, vol. 11, Nro. 1, 2013, Págs. 62/72.

podría exigir a un juez respecto de cómo se procederá al acceso y aprehensión de los datos o archivos, como así también, sobre el software a utilizar?[456]*"*

6.3.3.3. Los límites como forma de garantía

Coincidimos con este autor acerca de la dificultad que puede llegar a existir al momento de esperar que las autorizaciones judiciales sean técnicamente minuciosas (tipo de exploit a utilizar, tipo de vulnerabilidad a atacar, tipo de técnica de phishing a realizar, etc.), toda vez que en definitiva todas estas cuestiones terminarán dependiendo de lo que el perito experto en informática o las fuerzas de seguridad especializadas le indiquen al juez que deba especificar en su orden, con independencia de los altos conocimientos informáticos que los magistrados puedan adquirir.

Sin perjuicio de la debida motivación de la medida, en cumplimiento con todos los principios desarrollados en este trabajo (especialidad, proporcionalidad, idoneidad, etc.) y, principalmente, la limitación del alcance de la medida, pues, dado el alto nivel de intrusión en la vida privada al que puede acceder el Estado mediante un registro remoto, es necesario que se determine antes de iniciar la medida qué se quiere buscar y se eviten criterios amplios de búsqueda como "todo aquello de interés para la causa"[457].

Además, acompañamos la idea sobre que la principal atención debería concentrarse en el minucioso control ex post de la cadena de custodia, que refleje el registro en forma completa y detallada de todos las tareas efectuadas por los informáticos/programas y el movimiento/manipulación de la evidencia. De este modo, las partes podrán controlar la integridad y resguardo de la evidencia obtenida.

A modo de cierre preliminar, entendemos que avanzar en esta clase de medidas debería en la práctica implicar la existencia de protocolos claros, que brinden transparencia (sobre todo para que la defensa pueda realizar sus

[456] STRATIOTIS, Diego: "Los allanamientos remotos y el uso de drones o robots", Disponible en: https://jusmendoza.gob.ar/wp-content/uploads/2022/06/Stratiotis-Diego.pdf
[457] STRATIOTIS, Diego: "Los allanamientos remotos y el uso de drones o robots", Disponible en: https://jusmendoza.gob.ar/wp-content/uploads/2022/06/Stratiotis-Diego.pdf

respectivos controles), por lo que sería importante avanzar en la generación de protocolos de actuación redactados por equipos multidisciplinarios (conformados por expertos informáticos, juristas y personal operativo de las fuerzas de seguridad) en los que se definan los aspectos básicos a tener en cuenta en las tareas de búsqueda, obtención, preservación, examen pericial y presentación de evidencias digitales, en miras a garantizar el registro de cada paso vinculado a la manipulación de la evidencia.

6.3.4. Identificación de dispositivo mediante captación de información de sistema

A modo general, esta técnica consiste en la recolección, procesamiento y análisis de un conjunto de información que expone un dispositivo o sistema determinado al conectarse a un servidor controlado por el investigador. Entre la información que puede ser captada de la interacción con un sistema o dispositivo, podemos mencionar el sistema operativo utilizado, su versión, navegador de internet utilizado, plugins instalados, fuentes instaladas en dicho sistema, resolución de pantalla utilizada por el dispositivo, dirección IP pública utilizada por la conexión a internet, modelo del dispositivo celular utilizado (en el caso que la conexión sea realizada desde un celular) hasta incluso, en algunos casos, la ubicación geográfica de la persona conectada.

Del conjunto de todos los datos que se puedan recolectar del dispositivo de interés (utilizado por la persona sospechosa, por ejemplo, en un caso de grooming), usualmente se procede a realizar un agrupamiento de este conjunto de datos, generando una "huella digital" de dicho usuario, que podrá ser de utilidad para determinar la identificación – con cierto nivel de precisión- de un dispositivo de conexión.

De la misma forma que algunas características de las personas (como la huella dactilar) permite su identificación unívoca, asimismo es posible realizar un proceso similar con los dispositivos. Si bien su nivel de precisión no es del 100%, sus niveles

suelen superar el 90%, como veremos en algunas de las técnicas analizadas a continuación.

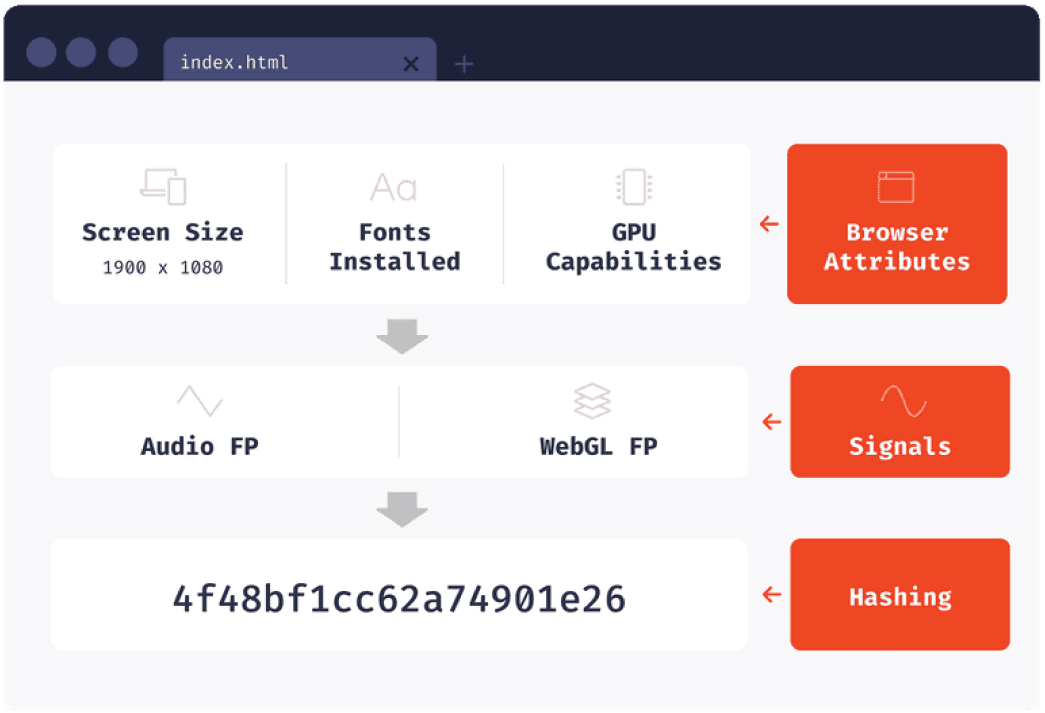
6.3.4.1. La técnica del Browser fingerprinting

Existen distintos tipos de técnicas que podrían dar lugar a la captación de esta información de identificación, pero no extendernos demasiado en el aspecto técnico, procederemos a realizar una referencia a una de ellas, conocida como browser fingerprinting.

Esta tecnología es de uso cotidiano por distintos portales y servicios web, para identificar a un usuario y observar su comportamiento en línea, para posteriormente poder "ajustar" el servicio a sus preferencias. Es decir, permitiría identificar a un mismo usuario, aunque el mismo cambie de dirección IP cada 5 minutos. Hace años que desde la Electronic Frontier Foundation (EFF), a través del proyecto *Panopticlick*[458], advierten sobre los peligros de la privacidad de la utilización de este tipo de técnicas de identificación de usuarios por parte de empresas privadas (uso comercial).

Actualmente, su utilización ha crecido notablemente en soluciones que ofrecen prevención de fraude, toda vez que permitiría detectar a un usuario fraudulento o que quiere tratar de afectar de alguna forma un servicio, a través de información que no tiene una relación directa con la dirección desde la cuál se conecta (entendiendo que probablemente puedan contratar servicios de VPN que permiten alternar entre distintas direcciones IP según su necesidad).

[458] Electronic Frontier Foundation: Panopticlick. Url: https://panopticlick.eff.org/about#browser-fingerprinting



Como muestra el gráfico anterior de una forma didáctica, la técnica consiste en recolectar distintos tipos de datos que pueden obtenerse de la conexión del usuario, generando un huella digital (hash) que permitirá a futuro, detectar a este mismo usuario.

De acuerdo a un estudio realizado por la EFF[459], en los navegadores compatibles con Flash o Java, es posible que en promedio se recolecta al menos 18.8 bits de información de identificación, **logrando un porcentaje de exactitud en la identificación del 94.2%.**

Según un estudio de la Agencia Española de Protección de Datos[460] existen numerosas propiedades que se pueden recopilar de un dispositivo a través del navegador web y que permiten recoger información suficiente para que, en determinadas situaciones, se pueda identificar unívocamente el terminal. Como se ha comentado anteriormente, algunas de estas características son ampliamente conocidas porque se vienen utilizando habitualmente para presentar las aplicaciones

[459] ECKERSLEY, Peter,, "How Unique Is Your Web Browser?", Electronic Frontier Foundation. Url: https://panopticlick.eff.org/static/browser-uniqueness.pdf
[460] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD); "Estudio Fingerprinting o Huella digital del dispositivo", Disponible en: https://www.aepd.es/documento/estudio-fingerprinting-huella-digital.pdf

o páginas web adaptadas al dispositivo que accede a ellas. Sin embargo, otras son mucho menos conocidas y pueden llegar a sorprender por su grado de sofisticación.

Dicho estudio posee un anexo con enorme listado de información que es posible extraer de una conexión, pero sin ánimo de exhaustividad, algunas de las características del terminal que se pueden recoger mediante el navegador web y que pueden contribuir a la obtención de una huella digital de un dispositivo como son el tipo, versión y configuración personal del navegador, los conjuntos de caracteres instalados que dan información sobre las aplicaciones instaladas, el idioma, zona horaria, configuración de pantalla y de elementos técnicos del terminal, dirección IP, etc. También se incluye información sobre otras técnicas más avanzadas que en condiciones normales permiten una mayor particularización del dispositivo como son canvas fingerprinting, canvas font fingerprinting, webRTC fingerprinting y audiocontext fingerprinting. Sobre estas últimas, a continuación daremos un breve detalle de funcionamiento en esta sección.

Además de las técnicas citadas anteriormente existen muchas otras propiedades que se podrían recoger y en algunos casos se utilizan para formar parte de la huella digital del dispositivo, como son: Instalación de bloqueadores de publicidad en el navegador; Memoria del dispositivo; Número de monitores conectados al dispositivo; Dispositivo con acelerómetro; Presencia de teclados virtuales; Lista de gestos soportados en el caso de dispositivos con pantalla multitáctil; Codecs de audio y video disponibles; Perfil de uso de la batería del terminal e incluso, hasta el listado de aplicaciones instaladas.

6.3.4.2. Canvas Fingerprinting

Se hace uso del elemento canvas de HTML5 para renderizar una determinada imagen mediante javascript. Esta imagen será renderizada de forma sutilmente diferente por las diferencias de hardware/software de cada dispositivo. Estas sutiles diferencias pueden detectarse al objeto de identificar los dispositivos.

HTML Canvas es un elemento que se utiliza para dibujar en tiempo real en páginas web utilizando código JavaScript que se ejecuta en el navegador del

usuario. El elemento Canvas es únicamente un contenedor para gráficos, se necesita hacer uso de lenguajes como JavaScript para dibujar en el contenedor. HTML Canvas tiene diferentes métodos que permiten dibujar líneas, rectángulos, arcos, texto y añadir imágenes.

Este elemento, HTML Canvas, se puede utilizar para hacer fingerprinting de usuarios. Diferencias en la renderización de fuentes, suavizados, antialiasing y otras características hacen que cada dispositivo dibuje la imagen de forma sutilmente diferente, lo que permite obtener una huella digital del usuario. El factor que forma parte de la huella digital del dispositivo es un hash de la imagen particular renderizada por el dispositivo[461].

6.3.4.3. WEBRTC

Esta técnica consiste en el uso de la API WebRTC de HTML5 para obtener la IP local (IP detrás de un NAT) de un dispositivo. La IP local en combinación con la IP pública constituye un factor de identificación del dispositivo muy consistente.

WebRTC es un framework libre y de código abierto que proporciona a navegadores y aplicaciones móviles capacidades de comunicación en tiempo real (Real-Time Communications RTC) p2p (peer to peer) entre dispositivos. Para determinar el mejor camino en la red entre los dispositivos, cada uno de ellos recoge información sobre las direcciones del otro, incluido direcciones IP de redes locales (Ethernet o WiFi) y direcciones del lado público del NAT, haciéndolas disponibles a la aplicación web sin el consentimiento explícito del usuario. Las aplicaciones web pueden acceder a las direcciones IP locales de los usuarios detrás de un NAT (Network Address Translation), y esta información es muy útil con fines de seguimiento. Pongamos el ejemplo de una red local con 20 dispositivos conectados a la red y a internet a través de un router. Una aplicación web podría acceder a la IP

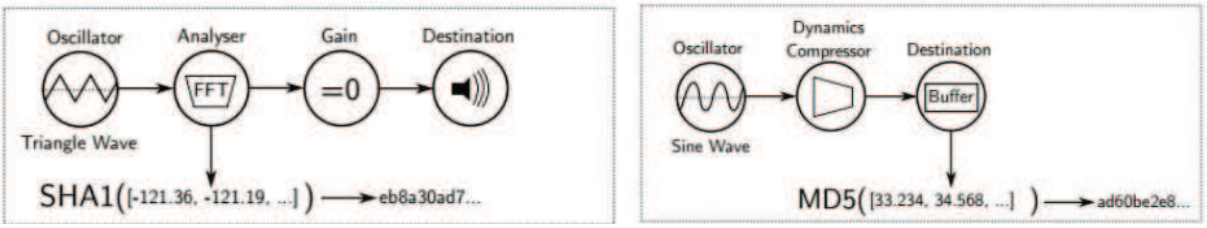
[461] MOWERY, Keaton y SHACHAM, Hovav; "Pixel Perfect: Fingerprinting Canvas in HTML5", Departamento de Ingeniería y Ciencias de la Computación de la Universidad de San Diego, California, EEUU; Disponible en: https://hovav.net/ucsd/dist/canvas.pdf

pública de la red/router y a la IP privada de cada uno de los dispositivos, pudiendo singularizar perfectamente cada dispositivo a pesar de estar detrás de un router[462].

6.3.4.4. AudioContext

Se utiliza la API AudioContext de HTML5 para realizar una serie de procesamientos sobre una señal de audio fija. Las ligeras diferencias en el resultado del procesamiento según el hardware/software del sistema concreto permiten particularizar el dispositivo.

Este tipo de técnica funciona de forma muy similar al Canvas Fingerprinting, pero utilizando audio en lugar de imágenes. Mediante la utilización de la librería AudioContext disponible en la mayoría de navegadores más recientes se pueden utilizar las sutiles diferencias de renderización de una señal de audio determinada, por ejemplo una señal sinusoidal o triangular, para generar una huella digital. Cabe reseñar que el uso de esta técnica no implica recoger señales de audio reproducidas o grabadas en el dispositivo, sino que se trata de una propiedad de la pila de proceso de audio del dispositivo.



Los dos métodos más utilizados para AudioContext fingerprinting se muestran en la Figura que acompañamos. Ambos métodos procesan una señal generada mediante un nodo de oscilación para luego leer la señal resultante y generar un hash que constituye la huella digital generada. La misma señal de audio procesada por

[462] ENGLEHARDT, Steven y NARAYANAN, Arvind, "Online Tracking: A 1-million-site Measurement and Analysis", Princeton University, Disponible en: https://dl.acm.org/doi/pdf/10.1145/2976749.2978313

distintos dispositivos o navegadores tendrá sutiles diferencias debido a las diferencias de hardware/software entre dispositivos[463].

6.3.4.5. Una herramienta a tener en cuenta

Dependiendo del tipo de caso que estamos investigando, esta técnica podría, al igual que otras revisadas anteriormente, ser de nula o gran importancia. Claro está que se parte de la base de la posibilidad de un contacto electrónico directo (chat por ejemplo) o indirecto (correo electrónico, posteos en redes sociales) con la persona investigada.

A nuestro criterio, entendemos que brinda importantes posibilidades de poder identificar información de interés y relevancia para una investigación (como por ejemplo, la dirección IP desde donde se conecta, el dispositivo celular que está utilizando, la versión del sistema operativo que tiene, etc.) que incluso, podrán ser insumos de importancia para la eventual ejecución de medidas más invasivas, como el registro remoto.

Desde el punto de vista jurídico, el Estado no estaría recolectando mayor información que lo hacen muchos de los sitios webs que utilizan esta misma tecnología (como cookies) para saber los hábitos de consumos de sus usuarios y poder establecer mejores estrategias de marketing orientados a las ventas. En este sentido, si bien es cierta que hay una obtención de datos relacionados a la conexión de la persona, entendemos que el nivel de afectación de la privacidad sería de bajo nivel, por lo que entendemos que no sería indispensable la autorización judicial para la ejecución de la medida, aunque siempre claro está, conseguir la autorización judicial brindará mayor nivel de seguridad jurídica para la investigación.

Nuevamente, al igual que otros temas, entendemos que esta técnica amerita un mayor nivel de desarrollo, que por motivos ya explicados, exceden el objeto de la presente tesis, pero que dejamos aquí, un llamado de atención a la persona lectora que pueda interesarse en la temática.

[463] QUEIROZ, Jordan y FEITOSA, Eduardo, “A Web Browser Fingerprinting Method Based on the Web Audio API”, The Computer Journal, Volume 62, Issue 8, August 2019, Pages 1106–1120, Disponible en: https://doi.org/10.1093/comjnl/bxy146

6.3.5. Acceso transfronterizo de datos

Hemos comentado anteriormente en esta tesis, que uno de los desafíos jurídicos más importantes aún pendientes, tiene que ver con aquellas investigaciones penales en las que resulta necesario el acceso a datos informáticos alojados en servidores ubicados físicamente en jurisdicciones diferentes a la de las autoridades que tienen a su cargo la investigación o sea en lugares en los que no cuentan con poderes jurisdiccionales.

Tal como hemos advertido en otros de los subtemas anteriores, nuevamente estamos ante un desafío cuya pretensión de abordaje en estas líneas sería demasiado pretencioso, por lo que nos limitaremos a explicar brevemente la problemática con una breve mención a algunas de las respuestas jurídicas que están sobre la mesa internacional, siguiendo el trabajo del profesor y especialista en Derecho Procesal Penal, Marcos Salt[464].

Nos parece adecuado comenzar mencionando que el abaratamiento de los costos en el almacenamiento de información en la nube, tiene como consecuencia que guardar datos en servidores en otros países ya no sea solamente una opción para grandes empresas, sino opciones accesibles a personas particulares (como pueden ser opciones como Drive, Dropbox, Icloud, etc.). El otro aspecto que complica la situación, es la dificultad técnica que tiene saber dónde están realmente los datos, toda vez que por motivos de economía de datos (por ejemplo, con el balance de cargas automático[465]), las empresas pueden ir migrando los datos de un país a otro de acuerdo a distintas variables económicas (por ejemplo, porque la electricidad es más barata en determinados lugares, o las condiciones climáticas son más favorables para los data center, etc.).

[464] Basado en el trabajo "Nuevos Desafíos de la evidencia digital. El Acceso transfronterizo de datos en los países de América Latina", del Dr. Marcos Salt.

[465] VMWARE; Balance de Carga por Software o por Hardware: https://www.vmware.com/es/topics/glossary/content/software-load-balancing.html#:~:text=El%20balanceo%20de%20carga%20aumenta,servidores%20no%20se%20est%C3%A1n%20utilizando.

El acceso -en el marco de una investigación penal- a datos alojados en extraña jurisdicción afecta uno de los pilares básicos del sistema penal: nada menos que la idea de soberanía nacional como base de la fijación de los poderes procesales de las autoridades de cada país y límite infranqueable de fronteras físicas para la actuación de la justicia de un país en otro.

6.3.5.1. ¿Violación del principio de territorialidad?

Algunos autores como Jack Goldsmith[466], sostienen que este tipo registros y secuestros de datos no implican una violación al principio de territorialidad. De la lectura del trabajo de este autor, él mismo reconoce que su línea argumentativa no pasa por sostener que no habrá límites a las búsquedas, sino que tales límites no son deducibles de normas del principio de territorialidad. De hecho, sostiene que uno de los límites a estos accesos transfronterizos, podrían ser las afectaciones a la privacidad o la libertad de expresión.

En el marco del trabajo del autor (escrito en 2001), destaca que el Convenio de Budapest (que tenía recién un año de vigencia) no brindaba soluciones adecuadas al problema de los accesos transfronterizos de datos. Afirma en su texto que los mecanismos de cooperación establecidos por la Convención sólo serán efectivos si existe consentimiento universal al tratado y que por lo tanto, tendrá poca influencia sobre los crímenes cometidos por países que no firmen el mismo. Destaca que para los propósitos actuales es que la Convención no autoriza búsquedas transfronterizas a distancia, ni siquiera en casos de emergencia o persecución.

Goldsmith está convencido que determinados ataques del cibercrimen a veces exigirá ataques remotos unilaterales y registros e incautaciones transfronterizas. Este autor afirma que la "soberanía territorial" nunca ha tenido un contenido definitivo, que nunca ha sido inmutable ni sacrosanto, y nunca ha prohibido todas las influencias externas dentro de las fronteras de una nación, destacando que a lo largo de la historia, las naciones han modificado sus puntos de vista sobre la significado

[466] GOLDSMITH, Jack, “The internet and the Legitimacy of Remote Cross Border Searches”, publicado en Public Law And Legal Theory Working Paper nro. 16, The Law School, University of Chicago, 2001.

de las fronteras territoriales y el significado de un "violación territorial" en relación a circunstancias internacionales, incluídos los cambios tecnológicos.

Para ir cerrando esta postura, mencionamos que en las bases de su línea argumentativa, Goldsmith considera que la analogía de comparar la invasión física de las fuerzas policiales hacia otro territorio con el acceso transfronterizo de datos, "no es convincente". A su criterio propone que las búsquedas se asemejan mejor a las órdenes del gran jurado y a la ejecución de técnicas de espionaje. Desde el punto de vista de este autor, las búsquedas transfronterizas remotas encajarían en la práctica aceptada desde hace mucho tiempo de funcionarios de una nación que actúan dentro de su territorio (o de funcionarios públicos) para extraer información de otro.

A nuestro criterio, entendemos que más allá del esfuerzo argumentativo de Goldsmith, adoptar esta postura por cualquier Estado para poder justificar el acceso transfronterizo de datos, puede derivar en el caso concreto, en la exclusión probatoria por parte del juez competente en la causa, pero a un nivel más general, podría implicar en problemas de índole internacional, e incluso en potenciales incumplimientos en diversos tratados internacionales que existen afirmando el principio de territorialidad.

Entendemos y adherimos a este autor en la necesidad de legitimar el acceso transfronterizo de datos, entendiendo que es una herramienta fundamental para la lucha contra el cibercrimen. Acordamos también que parece un poco excesiva la analogía de comparar el acceso transfronterizo con la irrupción de fuerzas policiales de un país a otro, por ejemplo, para la detención de una persona. No obstante, entendemos que es necesario continuar en la búsqueda de otros argumentos que permitan regular esta herramienta, para determinados casos y en determinadas circunstancias.

6.3.5.2. La afectación de la soberanía nacional

En una línea mucho más aceptada internacionalmente, el Dr. Marcos Salt[467] afirma que resulta evidente que los principios generales tradicionales vigentes en la región tanto para determinar la ley penal aplicable en materia penal como para determinar el poder jurisdiccional para la aplicación de medidas de coerción o la obtención de evidencia en diferentes países, no han sido adaptadas a los desafíos que presenta en ambas áreas la era digital. Ello resulta más evidente a partir de la revolución generada por internet y, más complejo aún, a partir del crecimiento de la tendencia a alojar la información (potencial evidencia en un proceso penal) en servidores ubicados en extrañas jurisdicciones o incluso en varios servidores ubicados en países indeterminados.

Este autor afirma que, de acuerdo al principio general de "soberanía nacional" que determina los principios que rigen la aplicación de la ley penal en el espacio (tanto la ley penal sustantiva como la procesal), los poderes procesales y las herramientas procesales de cada país para la investigación en entornos digitales sólo pueden ser utilizados por sus autoridades solamente en el marco de su territorio. Conforme a las normas vigentes en la región Latinoamericana, en los casos en que las autoridades advierten que las evidencias deben ser obtenidas en un país extranjero deberán requerirlas mediante los mecanismos de cooperación internacional que rigen la relación entre ambos países.

Entre las conclusiones alcanzadas por el maestro Salt, destacamos su afirmación que nos afecta regionalmente al sostener "*tanto en las legislaciones de los países de la región como en los convenios regionales de cooperación en materia penal regionales, tiene fuerte impronta el principio de "soberanía nacional" que determina los poderes procesales y las herramientas procesales de cada país para la investigación en entornos digitales sólo pueden ser utilizados por sus autoridades en el marco de su territorio (lex fori)".*

[467] SALT, Marcos; "Nuevos Desafíos de la evidencia digital. El Acceso transfronterizo de datos en los países de América Latina". Disponible en: https://aadproc.org.ar/pdfs/biblioteca_virtual/Congreso_2015/Ponencias%20Generales/Procesal%20Penal/SALT%2C%20Marcos.pdf

6.3.5.3. Casos autorizados según el Convenio de Budapest

A nivel internacional, el Convenio de Cibercrimen de Budapest, en su artículo 32[468], establece dos casos donde el acceso transfronterizo de datos estaría legitimado: a) Cuando estos sean de acceso público. b) Cuando se obtiene consentimiento lícito y voluntario de la persona legalmente autorizada a revelarlos.

Este último supuesto genera muchas dudas de interpretación que requieren sobre quién es la persona autorizada y sobre la posible afectación del principio de territorialidad y soberanía al "saltearse" toda intervención del Estado nacional en el que se encuentra el servidor que aloja la información que es requerida por las autoridades de otro Estado.

La Convención de Budapest reguló el tema de acuerdo a los consensos que los representantes de los países redactores pudieron alcanzar en el momento de su redacción y posterior aprobación. El texto de la Convención toma parte de las propuestas de la Resolución R (95) del Comité de Ministros del Consejo de Europa y de las discusiones y propuestas de los demás foros internacionales. Sin embargo, al momento de establecer normas con carácter vinculante para los Estados, limita las situaciones en las que admite las posibilidades de los Estados de acceder a datos en extrañas jurisdicciones (art. 19). La norma es clara en expresar que se trata de la posibilidad de acceder a un sistema informático conectado siempre que se pueda determinar que el sistema al que se accede desde el dispositivo original se encuentre también ubicado en el mismo territorio, lo que parece excluir la posibilidad de que la medida habilite una intervención transfronteriza. En el capítulo dedicado a la cooperación internacional, aunque de manera limitada, la Convención es el primer texto normativo internacional vinculante que logra plasmar situaciones de acceso transfronterizo de datos como excepciones al principio de territorialidad que, de acuerdo al texto de la propia convención internacional, prevé como criterio general

[468] En su redacción en idioma original: *Article 32 –Trans-border access to stored computer data with consent or where publicly available*
A Party may, without the authorization of another Party:
a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or
b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

de asignación de los poderes procesales (en el art. 22 sobre Jurisdicción y en el art. 25 sobre principios generales para la asistencia mutua). Los redactores del texto advirtieron con razón que en el futuro resultaría necesario ampliar los criterios que lograron plasmar y de hecho dejaron abierta la posibilidad de nuevos supuestos legítimos de acceso a los datos en extraña jurisdicción.

Las explicaciones de los redactores expresadas en el punto 293 del reporte explicativo son indicativas de las dudas que el tema generaba y aún genera: "*La cuestión de si una Parte puede acceder de forma unilateral a los datos informáticos almacenados en otra Parte sin solicitar la asistencia mutua fue una cuestión que examinaron detenidamente quienes redactaron el Convenio. Hubo un examen detallado de los casos en los cuales puede ser aceptable que los Estados actúen de manera unilateral y aquellos en los que puede no serlo. En última instancia, quienes redactaron el Convenio determinaron que no era posible todavía elaborar un régimen completo y vinculante desde el punto de vista legal que regule este campo. En parte, esto se debió a la falta de experiencias concretas respecto de este tipo de situaciones hasta la fecha, y, en parte, esto se debió a que se consideró que la solución adecuada a menudo es resultado de las circunstancias concretas de cada caso, lo que hace difícil formular normas generales. En última instancia, los redactores decidieron sólo enunciados en el artículo 32 de la Convención de las situaciones en las que todos coincidimos en que la acción unilateral es admisible. Acordaron no regular otras situaciones hasta el momento en que la experiencia ha ido obteniendo más y más debates pueden celebrarse a la luz de la misma. En este sentido, el Artículo 39, párrafo 3 establece que no se autorizan ni se excluyen otras situaciones.*". Este último párrafo de la nota ha sido interpretada como una indicación expresa de los redactores de que no excluían otras formas de acceso transfronterizo.

6.3.5.4. La necesidad de regular casos de urgencia

Uno de los puntos en común encontrados entre los autores, y con el cuál también adherimos es que considerar que sería recomendable regular la posibilidad del acceso transfronterizo de datos de forma directa para casos de urgencia. Claro

está que sería un buen debate considerar qué casos podrían considerarse de urgencia (¿afectación de la vida de una persona? ¿Integridad de menores de edad?).

Nos sumamos también a su preocupación por la búsqueda del equilibrio entre la eficacia de las investigaciones, la afectación de derechos humanos, y el intervencionismo que podría terminar ocurriendo sobre empresas proveedoras de servicios. Asimismo coincidimos en la necesidad de avanzar en la regulación normativa (tal como veremos que se ha realizado en una de la Provincias de Argentina en este capítulo) de los procedimientos para la realización de las medidas que signifiquen acceso transfronterizo.

Para finalizar con esta temática, sugerimos a la persona lectora, no pasar por alto la propuesta normativa realizada por la Provincia de Salta (Argentina), en su artículo 309 quater en relación a la extensión de registros, con la introducción de una gran novedad en el punto c, al habilitar el acceso transfronterizo de datos "*cuando no resulta posible determinar en forma certera, al momento de ejecución de la medida, la jurisdicción en la cual los datos están alojados*". Para mayor desarrollo de esta normativa, invitamos a leer los comentarios realizados en la sección destinada a la Provincia de Salta, Argentina, que podrán encontrarse en este mismo Capítulo.

6.3.6. Desbloqueo compulsivo de datos informáticos

Uno de los grandes desafíos que se enfrenta la justicia en la actualidad, viene relacionado con el aumento del cifrado de las comunicaciones y los datos almacenados, con algoritmos de cifrado que -hasta el momento- son casi imposibles de romper (descifrar) para los laboratorios forenses de los equipos judiciales[469].

En este contexto, la facilidad que existe en el acceso a herramientas de cifrado (algunas hasta gratuitas) sumado con que incluso algunos equipos traen cifrado por defecto (como suele suceder con la línea de equipos de la marca Apple[470]), generan

[469] KERR, O; Compelled Decryption and the Privilege Against Self-Incrimination, en "Texas Law Review", vol 97, n*4, 2019, p. 1.
[470] Todo Noticias; "La Justicia no logra desbloquear dos celulares de Sofía Clerici y busca un iPhone que trajo de España"; Url:

cada vez menos posibilidades para que los especialistas en informática forense puedan realizar sus extracciones de datos, y así la Fiscalía pueda determinar si los datos encontrados son útiles o no para la investigación en curso.

Si bien existen algunas empresas de renombre internacional que venden (a cifras millonarias) el crackeo de dichas medidas de seguridad, esta posibilidad técnica (por el aspecto económico) termina quedando sólo restringidas a causas de mucho interés judicial -y político[471]-. Cabría destacar que esta empresa privada, tampoco revela cuál ha sido el camino "científico" para poder acceder a dichos datos, por lo que dicho procedimiento de apertura compulsiva también ha recibido cuestionamientos desde la defensa penal.

En el caso del iPhone de San Bernardino[472], el terrorista tenía en su poder un iPhone 5c y el FBI tardó casi cuatro meses en conseguir saltarse su seguridad. Lo hizo gracias a la compañía israelí Cellebrite y le costó la nada despreciable suma de 900.000 dólares, según trascendió en diversos medios especializados.

En este contexto, y considerando que actualmente muchos de estos bloqueos en el cifrado ya no tienen una contraseña (en realidad la tienen, como segundo factor de acceso), sino que su puede operarse su desbloqueo (descifrado) a través de la detección de ciertos datos biométricos previamente cargados en el dispositivo, como el reconocimiento facial o bien, la detección de la huella dactilar[473].

6.3.6.1. Desbloqueo compulsivo en Estados Unidos

Ahora bien, en este punto debemos realizarnos la pregunta clave del tema: ¿Es posible que el Estado pueda, a través de una medida coactiva, el desbloqueo compulsivo del equipo a través del uso de datos biométricos?.

---

https://tn.com.ar/politica/2023/12/04/la-justicia-no-logra-desbloquear-dos-celulares-de-sofia-clerici-y-busca-un-iphone-que-trajo-de-espana/

[471] DIARIO EL CIUDADANO WEB; "Teléfonos a San Pablo - Causa Sain: enérgica oposición al envío de celulares para desbloquear en Brasil"; Url: https://www.elciudadanoweb.com/causa-sain-energica-oposicion-al-envio-de-celulares-para-desbloquear-en-brasil/

[472] ELECTRONIC PRIVACY INFORMATION CENTER (EPIC); Apple vs. FBI; Disponible en: https://epic.org/documents/apple-v-fbi-2/

[473] KERR-SCHNEIER; Encryption Workarounas, en "Georgetown Law Journal", vol. 106, n*4, 2018, ps. 994 y ss. y 1003 y siguientes.

Jonathan Polansky ha desarrollado impecablemente este tema con su libro[474] un profundidad que excede el ámbito de esta tesis, pero a la cuál remitimos haciendo unas breves referencias a su importante trabajo relacionado con estas medidas y la posible afectación de garantías constitucionales que puedan ocurrir en el camino.

Para comenzar, expresamos que no nos resulta extraño encontrar que en Estados Unidos, distintos jueces[475] han determinado que las autoridades estatales pueden obligar a una persona a desbloquear su teléfono celular a través del ingreso compulsivo de sus datos biométricos y que esto no implica una violación a la 5ta. Enmienda de su Constitución Nacional (que consagra la garantía contra la autoincriminación), ya que se consideró que tal desbloqueo resultaba equiparable a una extracción compulsiva de ADN[476] o de huellas dactilares, medidas a las que tradicionalmente su jurisprudencia no les ha reconocido la protección de la garantía contra la autoincriminación por carecer de contenido declarativo[477]. La falta de extrañeza a nuestro criterio radica en que Estados Unidos posee una tradición mucho menos proteccionista de la intimidad y privacidad de las personas, aspectos que puede ser rápidamente corroborado con la laxitud -y hasta carencia- de normativa que busque garantizar la protección de datos personales, en clara contradicción con lo que ocurre en Europa a partir de numerosas normativa, pero sobre todo, del nuevo Reglamento Europeo de Protección de Datos[478].

6.3.6.2. Desbloqueo compulsivo en Argentina

En Argentina podemos encontrar que la garantía contra la autoincriminación se encuentra consagrada en el art. 18 de nuestra CN, que establece que "*nadie puede*

---

[474] POLANSKY, Jonathan, "Garantías constitucionales del procedimiento penal en el entorno digital"; 1º Edición, Editorial Hammurabi. 2020

[475] Ver Sentencia "Commonwealth v. Baust", caso n*CR-14-1439, resuelto por el Segundo Circuito Judicial del Estado de Virginia el 28/10/14.

[476] Ver Sentencia "Schmerber v. California", 384 U.S. 757, 764, resuelto por la Corte Suprema de Justicia de Estados Unidos el 20/6/66.

[477] Ver Sentencia "Hamilton - Winton", The government wants your fingerprint to unlock your phone. Should that be allowed?, en "Los Angeles Times", ejemplar del 30/4/16, disponible en www. latimes.com/localllcalifornialla-me-iphones-fingerprints-20160430-story.html

[478] REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016

ser obligado a declarar contra sí mismo". Esta garantía constituye un límite al objetivo de averiguar la verdad histórica, sobre el cual se estructura nuestro sistema procesal penal"[479]. El profesor Maier explica que esta acción implica que la declaración del imputado debe ser completamente voluntaria y libre, por lo que en caso de que alguna de estas condiciones no se vea cumplida en la declaración, esa únicamente podrá ser considerada en beneficio del imputado.

El derecho a no autoincriminarse, no obstante, se limita a las situaciones en las que la persona, a través de su relato, incorpora a la investigación evidencia del hecho objeto de la pesquisa". Afirma el profesor Maier[480] que no incluye aquellas en las que la persona es, en sí misma, un objeto de prueba, por ejemplo, cuando se extrae de ella una muestra de sangre para analizarla.

Como afirma Carrió, "*la doctrina y la jurisprudencia argentinas han delimitado el amparo de la garantía contra la autoincriminación a aquellos actos que poseen contenido comunicacional por parte del imputado, es decir, en términos de la jurisprudencia norteamericana, a los que resultan testimoniales*"[481].

El profesor Alejandro Carrió destaca sobre el tema el caso "Cincotta"[482], donde la Corte consideró que "*obligar a una persona a colocarse en una rueda de presos con fines identificatorios no resultaba violatorio de la garantía contra la autoincriminación, ya que esa acción no requería, por parte del imputado, la exteriorización de ningún tipo de comunicación*".

En el caso "H. G.S. y otro"[483], la Corte Suprema de Justicia de la Nación consideró que la extracción compulsiva de sangre de quienes resultaban ser potenciales imputados de un delito no violaba la garantía contra la autoincriminación. Fundamentó la decisión indicando que el art. 18 de la CN prohíbe obtener compulsivamente comunicaciones de las personas, o expresiones que debieran provenir de su libre voluntad; pero que la extracción compulsiva de sangre resultaba una evidencia de índole material, que no quedaba amparada por la garantía. En este

[479] MAIER, J. "Derecho procesal penal I. Fundamentos", 2º Ed., 2004, ps. 663 y 664.
[480] MAIER, J. "Derecho procesal penal I. Fundamentos", 2º Ed., 2004, p. 675.
[481] CARRIÓ, A.; "Garantías constitucionales en el proceso penal", 6º Ed., 2015, ps. 485 y 486.
[482] CSJN-Fallos, 255:18.
[483] CSJN-Fallos, 318:2518;LL, 1996-B-434; ED, 158-443; y Carrió, Garantías constitucionales en el proceso penal, 6* ed., 2015, ps. 531 y 532.

caso se investigaba la presunta apropiación de un menor de edad durante la última dictadura cívico-militar.

A modo de confirmación de esta postura, el Código Procesal Penal Federal, aprobado por la ley 27.063 y sus modificatorias, recepta estos criterios. Así, en el art. 175[484] se autoriza la extracción compulsiva de sangre, saliva, piel, cabello, etcétera, para la identificación o para obtener evidencia necesaria para la investigación. En el art. 177 se autoriza a que se obligue a un imputado a participar en una rueda de reconocimiento. Finalmente, en el art. 181 se autoriza a realizar exámenes corporales de un imputado, aun contra su voluntad, siempre y cuando eso no afectara su dignidad.

6.3.6.3. La existencia o no del contenido comunicacional

Como podemos observar, el derecho argentino en principio parece optar en este tema por postura similar al norteamericano en lo que respecta a los actos amparados por la garantía contra la autoincriminación. La cuestión central para definir el alcance de esta garantía es determinar si la medida probatoria posee contenido testimonial (en la Argentina llamado "comunicacional") por parte del imputado o no. La jurisprudencia de momento parece inclinarse que el desbloqueo compulsivo de los datos informáticos, no implica que sea un acto de contenido testimonial / comunicacional.

Jonathan Polansky desarrolla su postura en base a la postura opuesta, es decir, considera que el desbloqueo compulsivo sí debería considerarse como un acto comunicacional / testimonial. En su línea argumentativa reconoce que hacer que el imputado coloque uno de sus dedos de la mano en un teléfono, o que permanezca cerca e inmóvil a una corta distancia de la cámara frontal del dispositivo (en el caso del desbloqueo por reconocimiento de iris, habría que aguardar a que el imputado abriera los ojos, algo que irremediablemente sucedería) resultan medidas mucho menos agresivas, y por lo tanto afectan en menor medida la dignidad del imputado

[484] ARTÍCULO 175.- Individualización de personas. Podrá ordenarse la obtención de ácido desoxirribonucleico (ADN) del imputado o de otra persona si ello fuere necesario para su identificación o para la constatación de circunstancias de importancia para la investigación. [...]

que la extracción compulsiva de sangre o la administración de un enema, lo que fue admitido por nuestra jurisprudencia[485].

Sin embargo, Polansky entiende e insiste en que el desbloqueo de celulares mediante el ingreso compulsivo de datos biométricos, a diferencia de todas las otras modalidades en virtud de las cuales se obtienen evidencias del cuerpo del imputado, podría poseer contenido testimonial implícito, toda vez que quién a través de su huella digital, rostro o iris logra desencriptar un teléfono está informando a las autoridades estatales que es el usuario de ese dispositivo, que tiene control sobre él y, por lo tanto (y salvo evidencia en contrario), que su contenido le pertenece[486].

Polansky afirma que el desbloqueo mediante el ingreso compulsivo de datos biométricos posee contenido testimonial implícito, toda vez que quien desbloquea un dispositivo otorga evidencia que le permite al Estado afirmar, con un alto grado de probabilidad, que él es su usuario y posee control sobre su contenido. Esta información implícita, a diferencia de lo que sucede con la extracción compulsiva de sangre y las otras medidas analizadas, reviste una relevancia superlativa a la hora de atribuir responsabilidad penal por un delito.

El autor sostiene la comparación que "*el resultado incriminante en la extracción de sangre surge del análisis de la muestra, en el que no interviene el imputado, y no de la extracción en sí. En el caso de los teléfonos, en el ejemplo dado, la evidencia incriminante vendría del análisis del télefono (por ejemplo, la lectura de los mensajes, lo que resultaría equivalente al análisis de la muestra en el caso de la extracción de sangre), pero también del mero desbloqueo (equivalente a la extracción en sí)*"[487].

La medida no resultaría violatoria de la disposición constitucional sólo en los casos en los que las autoridades estatales ya tienen, antes de su producción, conocimiento de quién utiliza y controla el contenido del teléfono. En este tipo de casos, la información implícita que se derivaría del desbloqueo compulsivo del

[485] CARRIÓ, A. "Garantías constitucionales en el proceso penal", 6º Ed., 2015, ps. 528 y siguientes.
[486] Tal como lo manifestó el primer juez interviniente en el caso "In the matter of the search warrant application", caso Nº 17M85.
[487] POLANSKY, Jonathan, "Garantías constitucionales del procedimiento penal en el entorno digital"; 1º Edición, Editorial Hammurabi. 2020

teléfono no aportaría evidencia nueva alguna. A lo sumo, ratificaría un conocimiento que los órganos encargados de la persecución penal ya tenían de antemano.

Esta clase de situaciones se enmarcaría en la denominada doctrina *foregone conclusion*[488], que opera, en Estados Unidos, como excepción a la protección de la garantía contra la autoincriminación. Básicamente, esta doctrina establece que la producción de una medida probatoria que resultaría violatoria de la garantía contra la autoincriminación resulta tolerable, desde una perspectiva constitucional, en aquellos casos en los que el Estado tiene conocimiento a priori de la información implícita que se derivaría de la producción de la medida. En el caso del desbloqueo de teléfonos celulares mediante ingreso compulsivo de datos biométricos, la medida resultaría tolerable constitucionalmente si el Estado, antes de proceder al desbloqueo, puede demostrar que conoce quién es su usuario y, por lo tanto, quién es el que posee el control sobre el contenido del dispositivo.

A modo de cierre y conclusión de este tema, el autor citado considera "*Desde mi punto de vista, la foregone conclusion se podría aplicar perfectamente en la Argentina. Esta excepción no hace más que otorgarle valor jurídico a un hecho de la realidad: lo que aparenta ser una confesión no lo es, dado que el Estado tiene conocimiento previo del contenido de ese acto. En consecuencia, si las autoridades estatales conocen quién es el usuario y tiene control sobre un teléfono celular, obligar a un imputado a desbloquearlo mediante el ingreso compulsivo de sus datos biométricos constituiría un acto similar a una extracción compulsiva de sangre, que, como se vio, resulta admisible en nuestra tradición jurídica*"[489].

6.3.7. Hallazgos casuales en la evidencia digital

El uso actual de la tecnología ha generado que la mayoría de las personas cuenten con un dispositivo electrónico que almacene datos digitalmente (computadora, teléfono celular, pendrive, etcétera). La evolución tecnológica y su

[488] KERR O, "Computer Crime Law", 3º Ed., 2013, p. 532.
[489] POLANSKY, Jonathan, "Garantías constitucionales del procedimiento penal en el entorno digital"; 1º Edición, Editorial Hammurabi. 2020

consecuente abaratamiento de los costos, hacen que por ejemplo, los teléfonos móviles tengan cada vez mayor capacidad de almacenamiento y por ejemplo, muchas personas ya no se preocupen por "borrar fotos por falta de espacio de almacenamiento" en sus propios dispositivos. Esto tiene como consecuencia un caudal cada vez más grande de información, que en el marco de una investigación penal, podría quedar expuesta a la investigación, y por lo tanto, cada vez mayores posibilidades de afectar esferas de privacidad de la persona investigada.

6.3.7.1. La necesidad de repensar la doctrina de la plain view

En este contexto, se dispara el desafío de los hallazgos casuales, un tema que no es nuevo en sí (teníamos jurisprudencia sólida en materia de hallazgos casuales de evidencia tradicional), pero que a la luz de la evidencia digital, necesita una nueva mirada. Entonces ¿Qué sucede si en el transcurso del análisis de los datos de un disco rígido se encuentran elementos que dan cuenta de la comisión de otros delitos (por ejemplo, evasión tributaria de otras empresas o tenencia de material de abuso sexual infantil? ¿Se los puede utilizar para iniciar una nueva investigación o ampliar el objeto de la que está en curso, en el marco de la cual se dictó la medida de registro y secuestro original?.

Es sencillo comprender la aplicación de la exclusión de elementos probatorios por la doctrina de la "plain view" en el mundo físico, es el objeto del allanamiento el que, naturalmente, indica de qué forma se debe desarrollarla medida. Por ejemplo, si la orden habilita a ingresar a un domicilio para encontrar un automóvil robado, quienes la ejecuten no podrían revisar válidamente un baño de la finca, en el cual no resulta razonable encontrar el rodado. En caso de que así lo hicieran, los elementos secuestrados por fuera de la orden deberían excluirse del procedimiento penal. En este aspecto, es la descripción particularizada del objeto de la medida la que previene que las órdenes de allanamiento se transformen en una habilitación en blanco y general para revisar completamente todo lo que esté al alcance de quienes la ejecutan, desbalanceando la relación establecida por nuestra Constitución entre los intereses de proteger la intimidad y perseguir los delitos.[490]

[490] CARRIÓ, A.; "Garantías constitucionales en el proceso penal", 6º Ed., 2015, ps. 382

Podemos encontrar regulación de esta doctrina a nivel físico en el actual Código Procesal Penal Federal de Argentina, donde establece en su art. 146[491] que "*Si en estricto cumplimiento de la orden de allanamiento se encontraren objetos que evidenciaren la comisión de un delito distinto al que motivó la orden, se pondrá en conocimiento del juez o representante del MINISTERIO PÚBLICO FISCAL interviniente quien, en caso de estimarlo adecuado, ordenará su secuestro. En el acta se dejará constancia explicativa sobre el lugar y la forma en que fueron hallados todos los objetos secuestrados. Practicado el registro, se hará constar en el acta su resultado, con expresión de las circunstancias útiles para la investigación. El acta será firmada por los concurrentes. Si alguien no lo hiciere, se harán constar los motivos.*"

6.3.7.2. Hallazgos casuales según jurisprudencia Argentina

Según Carrió[492], la jurisprudencia argentina sostiene que, para proceder de tal modo, se deben dar las siguientes condiciones: 1) los elementos deben ser hallados en un lugar sobre el cual resultaba razonable encontrar los objetos que motivaron el dictado de la medida original, y 2) su carácter ilícito debe poder ser percibido a simple vista.

La plain view doctrine, originaria de Estados Unidos, buscó desde sus comienzos tratar de equilibrar es armonizar dos intereses que, en principio, parecen contrapuestos: la necesidad de investigar los delitos y la de respetarla privacidad de

---

Constitución de la Nación Argentina. Claves para el estudio inicial de la norma fundamental, 2007, p. 116; y D'Albora, Código Procesal Penal de la Nación. Anotado. Comentado. Concordado, 9* ed., 2012, p. 404 y siguientes.

[491] *CPPFederal - ARTÍCULO 146.- Recaudos para el registro. La diligencia se realizará procurando afectar lo menos posible el derecho a la intimidad. El registro se circunscribirá al lugar específico sobre el que se sospecha que pudiera encontrarse el objeto de búsqueda y comprenderá exclusivamente los elementos que estén relacionados con ese fin. Si en estricto cumplimiento de la orden de allanamiento se encontraren objetos que evidenciaren la comisión de un delito distinto al que motivó la orden, se pondrá en conocimiento del juez o representante del MINISTERIO PÚBLICO FISCAL interviniente quien, en caso de estimarlo adecuado, ordenará su secuestro. En el acta se dejará constancia explicativa sobre el lugar y la forma en que fueron hallados todos los objetos secuestrados. Practicado el registro, se hará constar en el acta su resultado, con expresión de las circunstancias útiles para la investigación. El acta será firmada por los concurrentes. Si alguien no lo hiciere, se harán constar los motivos.*

[492] CARRIÓ, Garantías constitucionales en el proceso penal, 6º Ed., 2015, p. 403; y D'Albora, Código Procesal Penal de la Nación. Anotado. Comentado. Concordado, 9" ed., 2012, p.402 y siguientes.

los individuos. Tenemos claro que el juez o jueza, antes de autorizar el ingreso de autoridades estatales a un domicilio privado deberían constatar que en la investigación existan elementos suficientes para habilitar una medida de semejante carácter intrusivo, y que exista probabilidad de encontrar elementos vinculados al delito investigado en el lugar que se pretende ingresar. Bajo este paradigma, la autorización para acceder a un domicilio privado y secuestrar elementos tiene un límite claro: solo se pueden secuestrar los elementos vinculados al delito investigado, los cuales el juez consideró factible encontrar en el lugar al momento de autorizar la medida, y para encontrar tales elementos, las autoridades solo pueden revisar las áreas del domicilio en donde resulta razonable encontrar tales elementos. La medida debe desarrollarse de modo tal de no entrometerse en la privacidad de los individuos más allá de lo estrictamente necesario, para encontrar los elementos que se autorizó a buscar.[493]

En materia de jurisprudencia argentina, en el caso "Lazarte"[494], la Sala I de la Cámara Nacional de Apelaciones en lo Criminal y Correccional consideró que, si en el marco de una intervención telefónica dictada en una investigación por un delito determinado, se escucha información respecto de otro delito de acción pública, resultaría posible iniciar una nueva investigación, siempre y cuando se contara con impulso del Ministerio Público Fiscal. A su vez, en el caso "A. G.F. y otros", la Sala III de la Cámara Nacional de Casación Penal sostuvo que, ante el hallazgo de elementos incriminantes encontrados en una escucha telefónica no relacionados con el objeto que dio origen a la intervención, "la prevención no puede renunciar a investigar por propia iniciativa una notitia criminis descubierta mediante una intervención telefónica legalmente autorizada[495].

El autor Jonathan Polansky considera que la jurisprudencia sobre el análisis de material obtenido mediante escuchas telefónicas no resulta aplicable al acceso a información contenida en dispositivos de almacenamiento digital, toda vez que las

[493] MOSHIRNIA, Andrew:, "Separating hard fact from hard drive: a solution for plain view doctrine in the digital domain", en "Harvard Journal of Law 8. Technology", vol. 23, n*2, 2010, ps. 611 y 612
[494] Ver Caso "Lazarte", JJ, 2004-11-772, ante la Sala | de la Cámara Nacional de Apelaciones en lo Criminal y Correccional, cit. en Carrió, Garantías constitucionales en el proceso penal, 6* ed., 2015, p.477 y siguientes.
[495] Ver Caso "A.G.F y otros" (Lexis, Nº 135002448), ante la Sala III dela Cámara Federal de Casación Penal, cit. en Carrió, Garantías constitucionales en el proceso penal, 6* ed., 2015, p.478 y siguientes.

particularidades del entorno digital son diferentes a las de las intervenciones telefónicas.

6.3.7.3. La diferencia en la afectación de derechos

Acompañamos su postura coincidiendo que las características de los entornos digitales modernos hacen que el riesgo de exposición en la revisión de información digitalmente almacenada sea exageradamente más alto. En las intervenciones telefónicas, el Estado tiene acceso a conversaciones que se dan en un plazo determinado (desde que se ordena la medida hasta su fin), generalmente corto. La naturaleza de la información en juego es la misma: conversaciones que tiene el sospechoso.

En cambio, en el ámbito digital el Estado accedería a información privada producida por periodos prolongados de tiempo. En una computadora podemos encontrar datos privados que se fueron resguardando durante años o, incluso, décadas (en nuestra computadora, podemos tener fotos o archivos personales muy antiguos). La naturaleza de esta información, a diferencia de lo que sucede con las intervenciones telefónicas, es de la más variada (conversaciones por canales de chat, fotografías, historiales de búsquedas en Internet, datos de georreferenciación, etcétera). Es más, en el análisis forense digital, hasta incluso es posible conocer información que fue almacenada y borrada, con lo cuál aumenta las diferencias con la comparación de una intervención telefónica.

Orin Kerr va más allá de señalar este tipo de dificultades. Sostiene que la plain view doctrine, por sus características, no se puede aplicar al mundo digital. El autor señala que lo que esta doctrina permite es secuestrar elementos que se perciben a simple vista como ilegales y que se encontraban por fuera del objetivo de la orden de registro y secuestro. ¿Qué rol cumpliría la plain view doctrine? En el mundo físico, sería evitar el secuestro del objeto. Pero aquí en el mundo digital, el equipo que contiene información (computadora por ejemplo) ya ha sido secuestrada con la correspondiente autorización. La plain view doctrine no tiene lugar en este tipo de

casos toda vez que no puede prevenir que se secuestre algo que, previamente, se había autorizado a secuestrar[496].

Hacemos un alto en este punto, para agregar algo que, quizás a la fecha de redacción de este autor, no era tan común como lo es actualmente, y que consiste en la posibilidad de realizar la recolección de datos "en caliente", es decir, que el juez no autorice el secuestro de los equipos, sino solamente el secuestro de los datos. En estos casos, el planteo realizado por Kerr podría ser diferente.

Continuando con lo expresado por Kerr, sostiene que el desarrollo de la tecnología y el actual uso que las personas les dan a los dispositivos electrónicos, requieren la elaboración de una nueva doctrina. Así como la plain view doctrine sirve para limitar las facultades de secuestro de elementos de las autoridades en registros desarrollados en el mundo físico, esta nueva doctrina debe limitar las facultades de las autoridades de utilizar elementos encontrados en el entorno digital. Para esto propone reemplazar la plain view doctrine por la prohibición de utilizar cualquier elemento encontrado en un dispositivo de almacenamiento digital que no se encuentre estrictamente relacionado con el objeto de la medida original.[497]

6.3.7.4. La prohibición de utilizar archivos no relacionados con la medida

¿Qué significa para Kerr la prohibición de utilizar los archivos no relacionados con el objeto de la medida? El autor sostiene que esto implica la prohibición de darle cualquier tipo de relevancia en la investigación. En primer lugar, no se podrían utilizar para luego expandir la investigación en curso o iniciar una nueva. Tampoco se podrían usar para solicitar la ampliación de la orden de registro y secuestro original. No obstante, considera que puede haber excepciones, por ejemplo, que la información encontrada por fuera del alcance de la medida original, revelara la necesidad de preservar la vida o evitar la continuación de una grave afectación de derechos, la utilización de esa información resulta razonable y admisible.

[496] KERR, O; Executing warrants for digital evidence: the case for use restrictions on nonresponsive data, en "Texas Tech Law Review", vol. 48, n* 1, 2015, p.21 y siguientes.
[497] op. cita anterior

Polansky sostiene[498] que la propuesta de Kerr, además de generar incertidumbre, consagra un derecho procesal de dos velocidades. Para determinados delitos, la garantía contra intromisiones arbitrarias del Estado (es decir, la utilización de elementos respecto de los cuales el Estado no tenía una orden previa de encontrar ni utilizar) estaría justificada, y para otros, no. Es decir, para algunos delitos regirían determinadas garantías constitucionales del procedimiento penal y para el resto, otras.

A nuestro criterio, habría que incorporar a la mesa de discusión el hecho que, como hemos ya comentado anteriormente en esta tesis, actualmente la saturación de trabajo de los laboratorios de informática forense (porque existen cada vez más dispositivos secuestrados de interés en diversas causas, pero también, porque el Estado no realiza las inversiones necesarias para dar respuesta a ese nuevo nivel de demanda) está incentivando que los mismos realicen meras operaciones de extracción de información, sin realizar los dictámenes periciales correspondientes.

Esta situación, de enviar las copias de la información para que funcionarios de la Fiscalía interviniente accedan a los datos y determinen si existe o no información de interés para la causa, termina siendo un enorme caldo de cultivo para el tema que estamos intentando abordar en esta sub sección. Es decir, más que nunca, se están accediendo a datos informáticos que no sólo vulnerar la privacidad e intimidad de las personas investigadas, sino que además, se corre el potencial riesgo que en esa expedición de búsquedas (sin limitaciones), se termine dando con información que pueda dar lugar a otra acción penal.

Volviendo un paso hacia atrás, estamos convencidos que si los laboratorios forenses tuvieran la posibilidad (técnica y humana) de realizar los dictámenes informático forense, basado en las preguntas periciales concretas que la fiscalía (y la defensa) realicen, la problemática de los hallazgos casuales se reduciría drásticamente, toda vez que los peritos informáticos ejecutan sus búsquedas y respuestas basados en procedimientos técnicos, disminuyendo la posibilidad de acceder a información por fuera de aquella que se de interés para la causa en curso.

[498] POLANSKY, Jonathan, "Garantías constitucionales del procedimiento penal en el entorno digital"; 1º Edición, Editorial Hammurabi. 2020

A nuestro humilde criterio, mejorar la práctica judicial en lo desarrollado anteriormente, sería un gran punto de partida. No obstante, frente a este tema de los hallazgos casuales, consideramos de importancia:

1. Que, al momento de autorizar el allanamiento, el juez o jueza definan con precisión los dispositivos o información de interés (por ejemplo, nombres de empresas, palabras clave determinadas involucradas en la causa, nombres de personas, etc.)
2. Que, al momento de realizar el allanamiento, asistan especialistas en recolección de evidencia digital, que disminuyan el exceso al momento de recolectar datos.
3. En el marco del laboratorio forense, si se secuestraron dispositivos, evitar las extracciones completas, tratando que la información extraída tenga algunos límites concretos.
    a. Por ejemplo, en una causa por lavado de dinero, restringir la extracción de información a archivos de ofimática (documentos, planillas, pdf, etc.), evitando así por ejemplo, extraer fotos y videos que podrían afectar la intimidad de la persona.
    b. Otro ejemplo, sería que el juez autorice la extracción de los datos, borrando toda la información que sea anterior o posterior a una determinada fecha[499].
4. Evitar el envío de los datos secuestrados a Fiscalía, concentrando la producción de los informes informáticos forenses en el laboratorio forense, fomentando la generación de puntos periciales concretos y precisos.
5. En el caso que el perito informático forense, desarrollando las técnicas necesarias para cumplir con lo autorizado por el juez o jueza. Uno de los puntos periciales, podría decir concretamente que si al momento de realizar

[499] En un caso real en el que hemos formado parte, como delegados técnicos de parte ejecutamos este tipo de medidas que fue autorizada por el juez de la causa. Concretamente, como se investigaba un delito económico puntual, y ya había sentencia anterior sobre la inocencia del acusado hasta una determinada fecha, el juez autorizó el borrado de toda la información anterior a la fecha del nuevo delito investigado. También, se autorizó el borrado de las conversaciones con los abogados. Técnicamente, se realizó una extracción completa del equipo, y luego en presencia del perito oficial de la fuerza de seguridad designada, se implementaron los borrados autorizados, en un tiempo de trabajo no mayor a 15 minutos. El resultado de la extracción recortada, fue enviado a la Fiscalía para su análisis.

su labor pericial, en el marco de un procedimiento técnico concreto, accede a información que a su criterio pueda implicar prueba de ese delito u otro delito diferente, la misma deberá ser notificada a la Fiscalía para su consideración.

Capítulo VII: Medidas de Investigación previstas en el Derecho Procesal Penal

7.1. Introducción:

Teniendo ya abordado el panorama internacional, es momento de avanzar sobre las medidas de investigación penal reguladas en los distintos países alcanzados por nuestro estudio.

Previamente, debemos realizar una advertencia metodológica previo a comenzar el presente análisis. Considerando entonces la extensión de algunos países como Brasil (26 Estados y el distrito federal) o México (31 estados y un distrito federal), advertimos a la persona lectora que se hace de extrema dificultad poder realizar una revisión particular de todos los estados internos, al menos con el nivel de rigurosidad académica que una tesis de doctorado requiere.

Por todo lo expuesto, hemos considerado que de los países alcanzados en el estudio, Argentina será el único país donde ha sido posible avanzar sobre una investigación particular sobre regulaciones existentes en distintas provincias. Dicha profundidad en la investigación ha tenido una relación directa con la posibilidad de acceso a información de estas provincias, así como el conocimiento particular de la realidad del interior de Argentina, considerando que este autor se encuentra radicado en la Ciudad de Santa Fe, Provincia de Santa Fe.

En el resto de los países alcanzados por el estudio (Brasil, Colombia, México y España) nos limitaremos en materia procesal penal a realizar una revisión sobre la normativa procesal penal existente a nivel federal o nacional.

Por otro lado, previo a realizar la investigación sobre derecho comparado en materia procesal penal, debemos realizar la aclaración sobre la interpretación de la aplicabilidad de las medidas encontradas.

De forma similar de lo que expuesto en la parte sustancial de esta tesis (Capítulo IV), donde para considerar la tipificación de un delito informático, se buscó el mayor nivel de coincidencia posible, y en aquellos casos donde no se encontraba del todo, hicimos la aclaración sobre que el tipo penal encontrado nos parecía parcialmente aplicable, en el caso procesal penal, buscaremos replicar la misma metodología.

Vale decir, que el criterio para considerar si la medida es o no aplicable, será subjetivo, por lo que aclaramos que será a criterio de este autor considerar la parcialidad en la aplicación de la misma. No aclaramos en qué porcentaje nos parece que es parcialmente aplicable, que sería un análisis demasiado riguroso para el tipo de investigación que estamos buscando.

Volvemos a destacar como desafío de esta investigación, que en la búsqueda de medidas de investigación reguladas, nos encontramos con la diversidad de tradición jurídica de cada país en particular, sumado a que en muchos casos, las medidas especiales de investigación, dejan de estar en el propio Código Procesal Penal para pasar a formar parte de normativas especiales.

7.1.1. Selección de medidas o técnicas de investigación

Destacamos que el presente estudio de derecho comparado, se realizará sobre las siguientes medidas de investigación, de las cuáles las primeras 6 han sido seleccionadas de las medidas sugeridas para ser reguladas por el propio Convenio de Cibercrimen de Budapest, entre las medidas a aplicarse dentro del territorio del Estado Parte (hemos excluído aquellas que tenían por destino medidas en cooperación con otros Estados Parte).

Adicionalmente, hemos incluído otras medidas o técnicas de investigación no incluídas en el Convenio de Budapest pero que, a nuestro criterio, son relevantes y tienen cada vez mayor nivel de trascendencia en el marco de las investigaciones penales que buscan la incorporación de evidencia digital al proceso, y que ya se pueden ver en algunas partes del mundo, casos incipientes de regulación para

algunas medidas (como OSINT) o bien, algunos casos donde existe mayor nivel de consenso, como lo son el agente encubierto digital o el registro remoto.

Dicho lo anterior, a continuación acompañamos el listado final de las medidas o técnicas de investigación a la cuál limitaremos el alcance del presente estudio de derecho comparado, configurando las siguientes 12 figuras:

Nº	Medidas de investigación reguladas en el Convenio de Cibercrimen de Budapest categorizadas de acuerdo a la posibilidad de aplicación dentro del territorio del Estado Parte
1	Conservación inmediata de datos informáticos almacenados (Artículo 16 C.C.Budapest.)
2	Conservación y divulgación inmediata de los datos de tráfico (Artículo 17 C.C.Budapest.)
3	Mandato de comunicación (Artículo 18 C.C.Budapest.)
4	Registro y decomiso de datos informáticos almacenados (Artículo 19 C.C.Budapest.)
5	Recogida en tiempo real de datos de tráfico (Artículo 20 C.C.Budapest.)
6	Interceptación de datos relativos al contenido (Artículo 21 C.C.Budapest.)
7	Agente encubierto Digital
8	Registro remoto
9	OSINT
10	Acceso transfronterizo de datos
11	Hallazgos casuales en evidencia digital
12	Desbloqueo compulsivo de datos informáticos

Tabla Nº 25: Resumen de medidas de investigación seleccionadas para realizar el estudio de derecho comparado

7.2. Medidas de investigación reguladas en Argentina

Es necesario comenzar señalando que Argentina es un país federal compuesto por 23 Provincias y la Ciudad Autónoma de Buenos Aires. Según nuestra Constitución Nacional, el código penal es una cuestión federal, sin embargo, el aspecto procesal penal tiene una regulación para casos federales (de excepción) y una regulación que ha quedado reservado por las Provincias, es decir, que depende del poder legislativo de cada Provincia.

Por lo tanto, sólo en Argentina, es posible encontrar 25 sistemas procesales penales: 1 sistema federal y 24 sistemas que pertenecen a CABA + 23 Provincias Argentinas.

En esta subsección, abordaremos la búsqueda de normativa que regule medidas de investigación relacionadas a la evidencia digital, en el ámbito federal primero, Ciudad Autónomas de Buenos Aires y luego iremos repasando sólo algunas Provincias Argentinas que han realizado importantes avances en la materia (Mendoza, Neuquén y Salta). Dejamos constancia entonces que en el resto de las Provincias Argentinas (20 Provincias restantes) han sido excluidas por considerar que tenían un nulo o casi nulo desarrollo en la materia de interés.

7.2.1. Código Procesal Penal Federal

La mala noticia en este aspecto, es que en Argentina a nivel federal, aún no se ha actualizado el Código Procesal Penal. Decimos aún, porque por ejemplo existieron propuestas que al menos, hasta la fecha donde podemos escribir estas líneas, nunca han podido llegar a cristalizarse en el CPPN.

7.2.1.1. Proyectos que no fueron

Un primer intento fallido de regulación existió en el frustrado Proyecto del Código procesal Penal de la Nación en el año 2007. Por medio del Decreto 115/2007, el Poder Ejecutivo Nacional decidió conformar una Comisión Asesora para realizar una reforma integral al Código Procesal Penal de la Nación. En 2010, se elevó el anteproyecto que en su artículo 181, incorporaba la medida de incautación de datos regulada de la siguiente manera "*el juez podrá ordenar, a requerimiento de parte y por auto fundado, el registro de un sistema informático o de parte de él, o de un medio de almacenamiento de datos informáticos o electrónicos con el objeto de secuestrar los componentes del sistema, obtener copia o preservar datos o elementos de interés para la investigación (…) aun antes de este requerimiento el fiscal podrá ordenar la conservación y protección de datos informáticos o electrónicos cuando existan razones para suponer que estos datos puedan ser perdidos o modificados. Esta medida podrá extenderse por un plazo de hasta noventa (90) días, a fin de obtener la orden judicial necesaria para su revelación*". Aparte de la mencionada, dicho proyecto no tenía muchas más incorporaciones de interés para el tema que nos ocupa, pero considerando el año de su propuesta, era bastante moderno.

Años más tarde, en el año 2014 existió un proyecto de reforma integral del Código Procesal Penal de la Nación[500], en el cuál se incluía el art. 144[501] sobre incautación de datos, donde incluía una regulación similar a la citada anteriormente. Nuevamente, aparte de esta medida de incautación de datos, del análisis del proyecto no encontramos otras medidas relacionadas a la obtención de evidencia

[500] Texto completo disponible en: http://www.saij.gob.ar/docs-f/proyecto/proyecto_codigo_procesal_penal_nacion.pdf

[501] *ARTÍCULO 144.- Incautación de datos. El juez podrá ordenar a requerimiento de parte y por auto fundado, el registro de un sistema informático o de una parte de éste, o de un medio de almacenamiento de datos informáticos o electrónicos, con el objeto de secuestrar los componentes del sistema, obtener copia o preservar datos o elementos de interés para la investigación, bajo las condiciones establecidas en el artículo 129. Regirán las mismas limitaciones dispuestas para el secuestro de documentos. El examen de los objetos, documentos o el resultado de la interceptación de comunicaciones, se hará bajo la responsabilidad de la parte que lo solicitó. Una vez secuestrados los componentes del sistema, u obtenida la copia de los datos, se aplicarán las reglas de apertura y examen de correspondencia. Se dispondrá la devolución de los componentes que no tuvieran relación con el proceso y se procederá a la destrucción de las copias de los datos. El interesado podrá recurrir al juez para obtener la devolución de los componentes o la destrucción de los datos*

digital, algo que, por el año de la propuesta, y la imperiosa necesidad en relación a la materia, implicaba el desaprovechamiento de una gran oportunidad.

En el año 2016, el Ministerio de Justicia y Derechos Humanos de la Nación envió al Senado un proyecto de ley tendiente a reformar el Código Procesal Penal de la Nación que fuera aprobado por la Ley N° 27.063, y cuya entrada en vigencia fue suspendida por el Poder Ejecutivo, en virtud de las "dificultades que suscitaba su implementación"[502].

Según se indica en los fundamentos de la iniciativa, las modificaciones procuraban "fortalecer los lineamientos que dieron sustento a la reforma aprobada en 2014" y así "adaptar el Código a la investigación y el juzgamiento de los delitos de competencia en la Justicia Federal", en el marco del traspaso de la Justicia Nacional al ámbito de la Ciudad. Dicho proyecto buscaba convertir al Código Procesal Penal "en la ley de enjuiciamiento criminal aplicable a los tribunales del fuero federal de la República Argentina y, con ello, a los delitos más graves y complejos del ordenamiento penal".

Entre los cambios más importantes de nuestro interés, se propusieron diversas medidas especiales de investigación como, por ejemplo, "el agente encubierto, el informante, la vigilancia acústica, la vigilancia de las comunicaciones, la vigilancia remota sobre equipos informáticos, la vigilancia por dispositivos de captación de imagen y por dispositivos de locación o seguimiento".

Sumado a ello, dejaba al arbitrio del juez el análisis de razonabilidad de las medidas a adoptarse, sobre todo en estos casos de especial gravedad. Aquí, conforme resalta Salt, se puede efectuar una crítica al mentado proyecto toda vez que termina dejando a la valoración judicial cuáles son los supuestos de delitos concretos de especial gravedad, a fin de efectuar la habilitación legal.

Realizado el repaso por los principales proyectos, procederemos a realizar la identificación de medidas que hemos logrado encontrar en el texto actualizado hasta la fecha del Código Procesal Penal Federal de Argentina.

---

[502] REVISTA PENSAMIENTO PENAL; "Proyecto de reforma al CPPN"; Disponible en: https://www.pensamientopenal.com.ar/legislacion/44332-proyecto-reforma-al-cppn

7.2.1.2. Cuadro de medidas de investigación reguladas

Nº	Medidas de investigación	Código Procesal Penal Federal
1	Conservación inmediata de datos informáticos almacenados (Artículo 16 Convenio de Budapest)	**No se encontró medida especial aplicable.**
2	Conservación y divulgación inmediata de los datos de tráfico (Artículo 17 Convenio de Budapest)	**No se encontró medida especial aplicable.**
3	Mandato de comunicación (Artículo 18 Convenio de Budapest)	**No se encontró medida especial aplicable.**
4	Registro y decomiso de datos informáticos almacenados (Artículo 19 Convenio de Budapest)	**ARTÍCULO 151.- Incautación de datos.** El juez podrá ordenar a requerimiento de parte y por auto fundado, el registro de un sistema informático o de una parte de éste, o de un medio de almacenamiento de datos informáticos o electrónicos, con el objeto de secuestrar los componentes del sistema, obtener copia o preservar datos o elementos de interés para la investigación, bajo las condiciones establecidas en el artículo 136. Regirán las mismas limitaciones dispuestas para el secuestro de documentos. El examen de los objetos, documentos o el resultado de la interceptación de comunicaciones, se hará bajo la responsabilidad de la parte que lo solicitó. Una vez secuestrados los componentes del sistema, u obtenida la copia de los datos, se aplicarán las reglas de apertura y examen de correspondencia. Se dispondrá la devolución de los componentes que no tuvieran relación con el proceso y se procederá a la destrucción de las copias de los datos. El interesado podrá recurrir al juez para obtener la devolución de los componentes o la destrucción de los datos.
5	Recogida en tiempo real de datos de tráfico (Artículo 20 Convenio de Budapest)	**No se encontró medida especial aplicable.**
6	Interceptación de datos relativos al contenido (Artículo 21 Convenio de Budapest)	**ARTÍCULO 150.- Interceptación.** Siempre que resulte útil para la comprobación del delito, el juez podrá ordenar, a petición de parte, la interceptación y secuestro de la correspondencia postal, telegráfica, electrónica o cualquier otra forma de comunicación o de todo otro efecto remitido por el imputado o destinado a éste, aunque sea bajo nombre supuesto.

		Se procederá de modo análogo al allanamiento. La intervención de comunicaciones tendrá carácter excepcional y sólo podrá efectuarse por un plazo máximo de TREINTA (30) días, pudiendo ser renovada, expresando los motivos que justifican la extensión del plazo conforme la naturaleza y circunstancias del hecho investigado. La solicitud deberá indicar el plazo de duración que estime necesario según las circunstancias del caso. El juez controlará la legalidad y razonabilidad del requerimiento y resolverá fundadamente. Rige para los magistrados, funcionarios, agentes y empleados que tengan participación activa en la intervención y/o responsabilidad sobre los elementos probatorios, el deber de confidencialidad y secreto respecto de la información obtenida por estos medios. Quienes incumplan este deber incurrirán en responsabilidad penal. Las empresas que brinden el servicio de comunicación deberán posibilitar el cumplimiento inmediato de la diligencia, bajo apercibimiento de incurrir en responsabilidad penal. Si los elementos de convicción tenidos en consideración para ordenar la medida desaparecieren, hubiere transcurrido su plazo de duración o ésta hubiere alcanzado su objeto, deberá ser interrumpida inmediatamente.
7	Agente encubierto digital	**No se encontró medida especial aplicable.**
8	Registro remoto	**No se encontró medida especial aplicable.**
9	OSINT	**Resolución 144/2020: "Protocolo General para la prevención policial del delito con uso de fuentes digitales abiertas";** Por la extensión del texto, remitimos al mismo en la url: https://www.boletinoficial.gob.ar/detalleAviso/primera/230060/20200602
10	Acceso transfronterizo de datos	**No se encontró medida especial aplicable.**
11	Hallazgos casuales en evidencia digital	**No se encontró medida especial aplicable.**
12	Desbloqueo compulsivo de datos informáticos	**No se encontró medida especial aplicable.**

Tabla Nº 26: Resumen de medidas de investigación reguladas en Argentina a nivel federal

Como se puede observar de la tabla, lamentablemente son escasas las medidas de investigación que se encuentran reguladas a nivel federal en Argentina. Tratando de realizar un repaso breve sobre las medidas encontradas, debemos mencionar el art. 151 sobre incautación de datos, con una fórmula bastante similar a

lo que se venía proponiendo desde hace varios años en Argentina. Básicamente, la medida afirma que "*el Juez podrá ordenar a requerimiento de parte y por auto fundado, el registro de un sistema informático o de una parte de éste, o de un medio de almacenamiento de datos informáticos o electrónicos, con el objeto de secuestrar los componentes del sistema, obtener copia o preservar datos o elementos de interés para la investigación, bajo las condiciones establecidas en el artículo 136*"[503].

De esta forma, se regulariza a nivel federal la incautación de datos, como una medida autónoma y diferente de la requisa o secuestro tradicional de objetos. Es interesante destacar que prevé la posibilidad de la copia de datos, en vez del secuestro del equipo o sistema completo, algo que a los fines prácticos, es cada vez más utilizados en caso que sea posible su realización.

Por otro lado, destacamos que sobre el final del art. 151, se establece que "*Se dispondrá la devolución de los componentes que no tuvieran relación con el proceso y se procederá a la destrucción de las copias de los datos. El interesado podrá recurrir al juez para obtener la devolución de los componentes o la destrucción de los datos.*". Este aspecto también es importante toda vez que muchas veces los equipos informáticos secuestrados, luego de haber sido adecuadamente procesados (ya se le realizaron las extracciones de información a través de copias forenses por ejemplo), puedan ser restituidos a sus propietarios, entendiendo que -salvo casos de excepciones- dichos equipos pueden ser necesarios para el trabajo de una persona,

[503] *ARTÍCULO 136.- Inspección del lugar del hecho. No se podrán inspeccionar lugares y cosas, salvo que existiera motivo suficiente y fundado para presumir que se encontrarán elementos útiles para la investigación, conforme las reglas que establece este Código.*
De la diligencia se labrará un acta que será firmada por DOS (2) testigos que no pertenezcan a la fuerza de seguridad que llevó adelante el procedimiento y adicionalmente, por otro medio idóneo que garantice su inalterabilidad y fidelidad. Bajo esas formalidades, podrá ser incorporada al juicio con posterioridad a que quienes hubieran intervenido en la diligencia hayan sido interrogados por las partes y con el acuerdo de éstas.
Las fuerzas de seguridad serán las encargadas de realizar la diligencia, sin perjuicio de la presencia del representante del MINISTERIO PÚBLICO FISCAL en los casos en que éste la considerase oportuna.
Para realizar inspecciones o registros, podrá ordenarse que durante la diligencia no se ausenten quienes se encuentran en el lugar o que cualquier otra persona comparezca inmediatamente.
Los que desobedezcan podrán ser compelidos por la fuerza pública, según lo previsto en este Código. La restricción de la libertad no durará más de SEIS (6) horas sin recabar la orden del juez.

como sucedió en el caso del investigador en ciberseguridad argentino Javier Smaldone[504].

Asimismo, en el caso que se hayan realizado copias o extracciones de datos que, luego de su análisis se concluye que no son útiles o no tienen información relevante para la investigación en curso, los mismos deberían ser destruídos. La destrucción real de datos informáticos, es un proceso de muy difícil comprobación técnica para la persona afectada, por lo que siempre celebramos la existencia de laboratorios forenses que brinden transparencia sobre la vida útil de los datos.

En segundo lugar, encontramos una normal relacionada con la realización de interceptación de comunicaciones del art. 150, que si bien es una norma genérica (ya que describe tanto las comunicaciones postales, telegráficas y electrónicas) destacamos la existencia de un límite de 30 días máximo para la práctica de la medida, y la mención expresa para que el juez controle la legalidad y razonabilidad del pedido.

7.2.1.3. La regulación del OSINT en contexto de pandemia

Entre los aspectos más novedosos que hemos encontrado a nivel federal, que si bien no se encuentra dentro del Código Procesal Penal Federal, si se puede encontrar en la Resolución 144/2020[505] del Ministerio de Seguridad de la Nación Argentina, la cuál resuelve en su art. 1 aprobar el "PROTOCOLO GENERAL PARA LA PREVENCIÓN POLICIAL DEL DELITO CON USO DE FUENTES DIGITALES ABIERTAS" que forma parte integrante de dicha medida a través de un anexo.

Debemos mencionar que técnicamente es una normativa que no se encuentra vigente, toda vez que en el propio art. 1 se estableció que su vigencia dependía de la emergencia pública en materia sanitaria (contexto COVID-19). No obstante, como normativa es una referencia importante que vale la pena destacar por su contenido regulatorio en relación a la utilización de las fuentes digitales abiertas.

[504] FUNDACIÓN VÍA LIBRE: "Comunicado: organizaciones de derechos humanos rechazan medidas arbitrarias contra el investigador en seguridad digital Javier Smaldone"; Disponible en: https://www.vialibre.org.ar/comunicado-organizaciones-de-derechos-humanos-rechazan-medidas-arbitrarias-contra-el-investigador-en-seguridad-digital-javier-smaldone/

[505] Disponible en: https://www.boletinoficial.gob.ar/detalleAviso/primera/230060/20200602

También es clave destacar que, como se establece en el objeto (art. 1 del Anexo), la finalidad de la misma es cooperar con la prevención del delito que se desarrolla en el espacio cibernético. Según el art. 2 del anexo, se entiende por "fuentes digitales abiertas" a los medios y plataformas de información y comunicación digital de carácter público, no sensible y sin clasificación de seguridad, cuyo acceso no implique una vulneración al derecho a la intimidad de las personas, conforme lo normado en la Ley de Protección de Datos Personales N° 25.326 y sus normas reglamentarias.

7.2.1.4. Ciberpatrullaje pero con principios

Entre los aspectos positivos del Protocolo[506], destacamos la redacción de principios de actuación, en el Capítulo II, art. 7, entre los que se enumeran algunos principios que ya hemos repasado en el capítulo anterior de la presente tesis -legalidad, proporcionalidad, razonabilidad y necesidad-, sumado a algunos más "modernos", entre los que nos parece de interés destacar su desarrollo:

> ***e. Principio de protección de la razonable expectativa de privacidad.*** *Las tareas de prevención deberán omitir aquellas conductas susceptibles de ser consideradas regulares, usuales o inherentes al uso de Internet y que no evidencien una intención de delinquir. Asimismo, se descartará toda posibilidad de acumulación de registros relativos a las personas, debiéndose proceder a su efectiva destrucción luego de concluida la actividad preventora.*
>
> ***f. Principio de protección de los datos personales.*** *El personal policial interviniente deberá ajustarse a lo normado en la Ley de Protección de Datos Personales N° 25.326, con particular atención respecto de aquellos datos considerados sensibles, que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual; y de las publicaciones efectuadas por niñas, niños y adolescentes.*
>
> ***g. Principio de protección de la libertad de expresión.*** *Los indicadores establecidos para las tareas de prevención del delito con uso de fuentes digitales abiertas cuidarán de no implicar una afectación a la libertad de expresión garantizada por los principios y normas*

[506] MINISTERIO DE SEGURIDAD DE LA REPÚBLICA ARGENTINA, Resolución 144/2020: "Protocolo General para la prevención policial del delito con uso de fuentes digitales abiertas"; Disponible en: https://www.boletinoficial.gob.ar/detalleAviso/primera/230060/20200602

constitucionales y convencionales y por los estándares elaborados por sus respectivos órganos jurisdiccionales de aplicación. Las tareas de prevención policial se llevarán a cabo con las salvaguardas necesarias para evitar el autocontrol discursivo y la autocensura resultantes de una vigilancia masiva, genérica e indiscriminada, de modo que se preserve el debate plural y el intercambio democrático de las ideas.

h. Principio de no criminalización de las protestas en línea. *La protesta a través de redes sociales no formará parte de ningún indicador delictivo establecido para las tareas de prevención policial del delito con uso de fuentes digitales abiertas.*

i. Principio de restricción de la discrecionalidad en el cumplimiento de las tareas preventoras. *El personal policial debe estar sujeto a un cuadro completo de lineamientos, prioridades, directrices, procedimientos y órdenes de servicio.*

j. Principio de profesionalización del personal afectado a las tareas de prevención del delito con uso de fuentes digitales abiertas. *El personal al que se asignen dichas tareas será especialmente formado con perspectiva de derechos humanos en entornos digitales, y capacitado en procedimientos, herramientas y metodologías adecuados a los principios establecidos en el presente Protocolo General.*

k. Principio de destrucción del material prevenido no judicializado. *Los datos colectados de fuentes digitales abiertas y registrados con fines de prevención policial se cancelarán cuando la prevención no hubiera dado lugar a actuaciones judiciales.*[507]

l. Principio de publicidad. *El MINISTERIO DE SEGURIDAD dará a conocer los alcances y limitaciones de las tareas de prevención policial del delito con uso de fuentes digitales abiertas, que surgen del presente Protocolo General.*

m. Principio de transparencia y rendición de cuentas. *Se propenderá a la publicación regular de la información relacionada con la cantidad de casos y personas prevenidos junto con la duración de dichas actividades; las redes sociales y sitios web en general que fueron relevados; y las herramientas y las metodologías utilizadas para cada caso investigado.*

n. Principio de control y de responsabilidad por el uso abusivo y violatorio. *Se controlará la estricta observancia de los lineamientos, prioridades, directrices, procedimientos y órdenes de servicio impartidas; y se sancionará administrativamente la vigilancia ilegal por parte del personal policial, sin perjuicio de las responsabilidades de orden penal y civil que pudieran asimismo corresponder.*

---

[507] Sobre este principio, recomendamos obtener mayor información en el Libro "Garantías constitucionales del procedimiento penal en el entorno digital", CAPÍTULO V: "EL DERECHO A QUE SE ELIMINE LA INFORMACIÓN DIGITAL SECUESTRADA NO RELEVANTE PARA LA INVESTIGACIÓN", de Jonathan Polansky, autor ya citado en esta obra.

A modo de reflexión sobre la inclusión de estos principios de títulos importantes, expresamos a modo de opinión personal que su real y adecuado cumplimiento sería vital para el resguardo de los derechos y garantías de la ciudadanía en general, pero que lamentablemente, en la práctica e implementación de este tipo de tareas, estos principios de nombres pomposos muchas veces terminan siendo sólo aportes teóricos que se quedan en las buenas intenciones, pero cuyo respeto en la práctica es bajo o nulo. Similar apreciación podría realizarse en relación con los principios del tratamiento adecuado de los datos personales, que en su mayoría no son cumplidos adecuadamente por los Responsables de Datos.

En el último artículo (art. 18) del Protocolo objeto de análisis, hacemos notar la regulación sobre la subsidiariedad de la aplicación de los principios, ya que se establece que: "*Los principios, criterios y directrices generales del presente Protocolo General serán de aplicación subsidiaria, en lo pertinente, a las tareas de investigación criminal que realizan los cuerpos policiales y fuerzas de seguridad como órganos auxiliares de la justicia, en tanto impliquen una doctrina compatible con las instrucciones que impartan los magistrados y permitan su mejor ejecución*".

Advertimos entonces, que todo lo positivo que hemos señalado sobre la inclusión de principios protectorios de los derechos a los ciudadanos, podrían ser "dejados de lado" por alguna supuesta incompatibilidad con las instrucciones impartidas por los magistrados, aspecto que consideramos criticable, toda vez que dichos principios deberían ser respetados en todos los casos (por eso se llaman principios).

7.2.1.5. La particular situación sobre retención de datos de tráfico en Argentina

Como hemos visto anteriormente, esta medida es aquella que obliga a las empresas prestatarias del servicio de internet a almacenar la información que sobre en su poder referida a los datos de tráfico de los usuarios y/o abonados del servicio que se encuentra prestando por un tiempo determinado. Implica obligar a las empresas a guardar dicha información por un lapso de tiempo específico y previo al

inicio de cualquier investigación para el caso que oportunamente sea requerida por alguna autoridad judicial o administrativa. Es una medida preventiva y por tanto su realización es previa a la comisión de un hecho delictivo[508].

Esta es la principal diferencia entre retención y conservación de datos de tráfico. Mientras esta última, debe ser mediante requerimiento expreso, en el marco de una investigación judicial concreta iniciada sobre datos ya existentes y almacenados, la retención es previa al inicio de alguna investigación y sobre los datos que se van produciendo, en tiempo real, independientemente si son requeridos por alguna autoridad en el marco de una investigación.

En Argentina se sancionó la ley 25.873, luego reglamentada por decreto 1563/04 , que modifica la ley 19.978 conocida como "ley de telecomunicaciones". Dicha ley impuso a los prestadores de servicios de telecomunicaciones la obligación de disponer de los recursos humanos y tecnológicos necesarios para la captación y derivación de las comunicaciones que transmiten, para su observación remota a requerimiento del Poder Judicial o el Ministerio Público de conformidad con la legislación vigente. También dispone que los prestadores de servicios deberán registrar y sistematizar los datos filiatorios y domiciliarios de sus usuarios y clientes y los registros de tráfico de comunicaciones cursadas por los mismos para su consulta sin cargo por parte del Poder Judicial o el Ministerio Público de conformidad con la legislación vigente, debiendo ser conservada por los prestadores de servicios de telecomunicaciones por el plazo de diez años.

Sin embargo, más allá del decreto 357/05 que suspendió la aplicación de la ley, en el año 2009 hubo un pronunciamiento con carácter erga omnes de la Corte Suprema de Justicia de la Nación (caso "Halabi"[509]) que declaró inconstitucional esta norma y su reglamentación. En este fallo la Corte nacional sostuvo que "sólo la ley puede justificar la intromisión en la vida privada de una persona, siempre que medie un interés superior en resguardo de la libertad de los otros, la defensa de la sociedad, las buenas costumbres o la persecución del crimen (Fallos 306:1892;

[508] NEME, Catalina F., "Una mirada actual en materia de regulación de retención de datos de tráfico y conservación rápida de datos informáticos" en DUPUY Daniela y KIEFER Mariana, "Cibercrimen" Editorial BdeF, Buenos Aires, 2017.
[509] CSJN, "Halabi, Ernesto v. Estado Nacional s/amparo", 24/02/2009, cita online: 70051373

316:703, entre otros). Es en este marco constitucional que debe comprenderse, en el orden del proceso penal federal, la utilización del registro de comunicaciones telefónicas a los fines de la investigación penal que requiere ser emitida por un juez competente mediante auto fundado (conf. art. 236, parte 2ª, CPPN., según el texto establecido por la ley 25760), de manera que el común de los habitantes está sometido a restricciones en esta esfera semejantes a las que existen respecto a la intervención sobre el contenido de las comunicaciones escritas o telefónicas. Esta norma concuerda con el art. 18, ley 19798 que establece que "*la correspondencia de telecomunicaciones es inviolable. Su interceptación sólo procederá a requerimiento de juez competente*".

Así, la Corte establece que para el examen de las intercepciones de las comunicaciones es necesario la aplicación de un criterio restrictivo de interpretación y en este sentido, dijo que lo que las normas de la ley 25.873 "*han establecido no es otra cosa que una restricción que afecta una de las facetas del ámbito de la autonomía individual que constituye el derecho a la intimidad, por cuanto sus previsiones no distinguen ni precisan de modo suficiente las oportunidades ni las situaciones en las que operarán las interceptaciones, toda vez que no especifican el tratamiento del tráfico de información de Internet en cuyo contexto es indiscutible que los datos de navegación anudan a los contenidos. Se añade, a ello, la circunstancia de que las normas tampoco prevén un sistema específico para la protección de las comunicaciones en relación con la acumulación y tratamiento automatizado de los datos personales. En suma, como atinadamente ha sido juzgado en autos, resulta inadmisible que las restricciones autorizadas por la ley estén desprovistas del imprescindible grado de determinación que excluya la posibilidad de que su ejecución concreta por agentes de la administración quede en manos de la más libre discreción de estos últimos, afirmación que adquiere primordial relevancia si se advierte que desde 1992 es la Dirección de Observaciones Judiciales de la SIDE, que actúa bajo la órbita del poder político, la que debe cumplir con los requerimientos que formule el Poder Judicial en orden a la interceptación de comunicaciones telefónicas u otros medios de transmisión que se efectúen por esos circuitos*".

Es importante destacar que la Corte se refiere a la inconstitucionalidad de esa norma de retención en virtud de los términos en los que fue regulada, pero no establece que cualquier norma que se legisle al respecto sería inconstitucional[510]. Es importante este último aspecto toda vez que a la fecha no ha vuelto a haber una ley en Argentina que regule esta temática

7.2.2. Ciudad Autónoma de Buenos Aires

La Ley N° 2303 de la Ciudad Autónoma de Buenos Aires aprobó en el 2007 un nuevo texto del Código Procesal Penal de la Ciudad Autónoma de Buenos Aires. Si bien dicha norma fue actualizada en diversas ocasiones hasta la fecha, en ninguna de ellas pudo observarse que la actualización o modificación haya tenido como foco u objetivo el tema que nos convoca.

A fin de continuar avanzando en la tarea de relevamiento de regulación procesal penal en nuestro país, no podíamos dejar de repasar la normativa de la Ciudad Capital de Argentina. A continuación presentamos los resultados alcanzados.

7.2.2.1. Cuadro de medidas de investigación reguladas

Nº	Medidas de investigación	Código Procesal Penal de la Ciudad Autónoma de Buenos Aires
1	Conservación inmediata de datos informáticos almacenados (Artículo 16 Convenio de Budapest)	**No se encontró medida especial aplicable.**
2	Conservación y divulgación inmediata de los datos de tráfico (Artículo 17 Convenio de Budapest)	**No se encontró medida especial aplicable.**
3	Mandato de comunicación	**No se encontró medida especial aplicable.**

[510] NEME, Catalina F., "Una mirada actual en materia de regulación de retención de datos de tráfico y conservación rápida de datos informáticos" en DUPUY Daniela y KIEFER Mariana, "Cibercrimen" Editorial BdeF, Buenos Aires, 2017

	(Artículo 18 Convenio de Budapest)	
4	Registro y decomiso de datos informáticos almacenados (Artículo 19 Convenio de Budapest)	**Artículo 96 - Prohibición de abrir correspondencia o inspeccionar datos privados.** Los integrantes de la policía y otras fuerzas de seguridad no podrán abrir la correspondencia que secuestren, ni inspeccionar datos privados contenidos en soporte informático, sino que la remitirán a la autoridad judicial o del Ministerio Público Fiscal competente; sin embargo, en los casos urgentes, podrán ocurrir al juez competente más cercano, el que le autorizará la apertura de considerarlo oportuno. Una vez conocido el contenido, el/la Juez/a podrán autorizar a los integrantes de fuerzas de seguridad la inspección de correspondencia y datos privados contenidos en soporte informático legalmente incautados, a los fines periciales. **Artículo 119 - Secuestro y clausura provisional:** El/la Fiscal, o el/la Juez/a cuando así lo requiera el cumplimiento de la garantías constitucionales en general o respecto de los elementos mencionados en el artículo 13 inc. 8de la Constitución de la Ciudad Autónoma de Buenos Aires, podrán disponer la requisa y/o el secuestro de las cosas relacionadas con el hecho, o aquellas que puedan servir como medios de prueba. En casos urgentes esta medida podrá ser delegada en las fuerzas de seguridad en la forma prevista para los registros. El/la Fiscal podrá ordenar, cuando fuere oportuno, la presentación de los objetos o documentos a que se refiere este artículo, con excepción de los elementos citados en el artículo 13 inc. 8 de la Constitución de la Ciudad Autónoma de Buenos Aires. Cuando para la averiguación de un delito sea indispensable la clausura de un local o la inmovilización de cosas muebles que por su naturaleza o dimensiones no puedan ser mantenidas en depósito, se procederá a asegurarlas, según las reglas precedentes. Cuando el secuestro fuera de documentos, equipos de computación u otro soporte informático, deberá guardarse reserva de su contenido con igual alcance que el previsto para la interceptación de correspondencia y comunicaciones. **Artículo 346 - Objetos decomisados**: Cuando se decomise algún objeto se le dará el destino que corresponda según su naturaleza, conforme la reglamentación. El/la Juez/a, a pedido de la Fiscalía, podrá adoptar desde el inicio de las actuaciones judiciales las medidas cautelares suficientes para asegurar el decomiso del o de los inmuebles, fondos de comercio, depósitos, transportes, elementos informáticos, técnicos y de comunicación, y todo otro bien o derecho patrimonial sobre los que, por tratarse de instrumentos o efectos relacionados con el o los delitos que se investigan, el decomiso presumiblemente pueda recaer. El mismo alcance podrán tener las medidas cautelares destinadas a hacer cesar la comisión del delito o sus efectos, o a evitar que se consolide su provecho o a obstaculizar la impunidad de sus partícipes. En todos los casos se deberá dejar a salvo los derechos

		de restitución o indemnización del damnificado y de terceros. El Ministerio de Justicia y Seguridad o el organismo que en el futuro lo reemplace reglamentará las cuestiones atinentes a la instrumentación y destino de los bienes o derechos sobre los que recaen las medidas cautelares.
5	Recogida en tiempo real de datos de tráfico (Artículo 20 Convenio de Budapest)	**No se encontró medida especial aplicable.**
6	Interceptación de datos relativos al contenido (Artículo 21 Convenio de Budapest)	**No se encontró medida especial aplicable.**
7	Agente encubierto digital	**No se encontró medida especial aplicable.**
8	Registro remoto	**No se encontró medida especial aplicable.**
9	OSINT	**No se encontró medida especial aplicable.**
10	Acceso transfronterizo de datos	**No se encontró medida especial aplicable.**
11	Hallazgos casuales en evidencia digital	**No se encontró medida especial aplicable.**
12	Desbloqueo compulsivo de datos informáticos	**No se encontró medida especial aplicable.**

Tabla Nº 27: Resumen de medidas de investigación reguladas en Ciudad Autónoma de Buenos Aires (Argentina)

Como se puede observar, casi no hemos encontrado en el Código Procesal Penal de CABA, normas específicas que regulen las medidas de investigación de nuestro interés.

Excepcionalmente, en relación a la medida del Registro y decomiso de datos informáticos, hemos encontrado tres artículos que si bien, no hacen una referencia específica sobre la medida, si poseen en su interior alguna referencia a datos informáticos.

7.2.2.2. Prohibición de inspeccionar datos privados

En primer lugar, el art. 96 regula una prohibición de abrir correspondencia o inspeccionar datos privados, apuntada hacia las fuerzas de seguridad, toda vez que dicha acción sólo podrá ser realizada previa autorización judicial. En esa regulación, se mencionan a "datos privados contenidos en soporte informático" como un ejemplo más, similar a la correspondencia, de información que posee este nivel de protección jurídica.

En segundo lugar, el ar. 119 sobre secuestro y clausura provisional, donde en el último párrafo se menciona que cuando el secuestro fuera "*de equipos de computación u otro soporte informático, deberá guardarse reserva de su contenido con igual alcance que el previsto para la interceptación de correspondencia y comunicaciones.*". Nuevamente, la finalidad buscada es reconocer una garantía de privacidad para los datos contenidos en soportes informáticos, pero no hace referencia puntualmente a una medida particular de investigación.

En tercer lugar, el art. 346 sobre objetos decomisados, establece que el o la Jueza, a pedido de Fiscalía, podrá adoptar medidas cautelares suficientes para asegurar el decomiso de los elementos informáticos, técnicos y de comunicación. Prima facie, podría aquí pensarse que podría encontrarse fundamento jurídico para pedir la conservación de datos, ya que lo que se regula básicamente es la posibilidad de adopción de actuaciones judiciales tendientes a que la prueba no se pierda.

Sin embargo, considerando que el artículo versa sobre objetos ya decomisados, a nuestro criterio, sólo sería aplicable a medidas que se puedan tomar "*desde el inicio de las actuaciones judiciales*" (del decomiso). A modo de ejemplo, se nos ocurre que en esta gama de medidas habilitadas podríamos encontrar medidas como llevar adelante el corte del suministro de la energía eléctrica (buscando evitar que en el momento del decomiso, se produzca la destrucción de datos), o bien, separar las personas de los equipos informáticos, con la misma finalidad. Incluso posterior al decomiso, podría pensarse en resguardar los elementos informáticos en lugares adecuadamente protegidos o preparados para evitar que los datos puedan ser afectados (en un depósito con jaula de faraday por ejemplo), o bien, en el caso

de dispositivos celulares, podría ser que se cuente con cables de bateria para evitar que los equipos se descarguen por completo y se apaguen -cuestión que podría obstaculizar la recuperación de datos si el dispositivo tuviera contraseña al encenderse-.

Para hacer algunos comentarios finales, nos parece adecuado citar algunas palabras de la Fiscal a cargo del Equipo Especializado en Delitos Informáticos de la CABA, Daniela Dupuy[511], quien reconoce en línea con lo anteriormente observado que "*Ni en el Código Procesal Penal de la Nación, ni en el Código Procesal de la CABA, está contemplada la posibilidad de que el juez o fiscal —según quien dirija la investigación— ordene, fundadamente, la conservación de datos cuando corran peligro de ser eliminados. Es fundamental que la orden sea precisa para no causar perjuicios a otros usuarios y el secreto de la medida, en especial para el titular de los datos, es imprescindible para el éxito de la investigación. Hoy, en las investigaciones, estas medidas se solicitan amparados en el principio de libertad probatoria, contemplado en los arts. 93, 106 y 107 de la ley procesal local. Pero al no estar reglamentada la obligación de responder en tiempo y forma por parte de los ISP, muchas veces las respuestas a nuestros requerimientos pueden llegar a destiempo, o no llegar. Esta disposición sólo autoriza a las autoridades competentes a impedir la supresión de los datos pertinentes, pero no obliga a los proveedores a transferir los datos*".

Como ya hemos visto, la obligación de conservar y transferir los datos (mandato de comunicación) se contempla en los arts. 16, 17 y 18 del Convenio sobre ciberdelincuencia. En relación de la necesidad de regular tanto la conservación como los mandatos de comunicación sobre datos informáticos, Dupuy afirma que "*Es una medida menos gravosa que permite a los jueces ordenar la presentación de elementos relacionados con el delito en lugar de ordenar su secuestro — y si bien la orden de presentación está prevista tanto en el art. 232 del CPPN como en el art. 113, párr 3 del CPPCABA, lo ideal sería la adecuación de la presentación, por parte de cualquier persona física o jurídica, de datos contenidos en*

[511] DUPUY, Daniela; "Desafíos procesales en la investigación de delitos informáticos", Libro: Informática y Delito: Reunión preparatoria del XIX Congreso Internacional de la Asociación Internacional de Derecho Penal (AIDP).

un dispositivo de almacenamiento informático que esté bajo su poder o control y al que pueda acceder."

7.2.3. Mendoza

Al momento de escribir estas líneas, el Senado de Mendoza (Enero 2024) aprobó por unanimidad una modificación al Código Procesal Penal (Ley Provincial Nº 6730) de dicha provincia (que ya había sido aprobado por la Cámara de Diputados durante el 2023), que incluye diferentes figuras que son de interés para el presente trabajo. La iniciativa tenía media sanción de la Cámara Alta, pero al ser modificada durante el tratamiento en comisiones de Diputados, volvió nuevamente al Senado en donde se convirtió finalmente en ley. Actualmente, pasó al Ejecutivo para su promulgación.

A fin de avanzar en la tarea de relevamiento de regulación procesal penal en la Provincia de Mendoza (Argentina) a continuación presentamos los resultados alcanzados, considerando como incluída la aprobación de la última norma comentada.

7.2.3.1. Cuadro de medidas de investigación reguladas

Nº	Medidas de investigación	Medidas de investigación aprobadas por la Cámara de Senadores y Diputados de Mendoza (pendiente promulgación de Ejecutivo) + otras medidas ya reguladas en el CPP Mendoza
1	Conservación inmediata de datos informáticos almacenados (Artículo 16 Convenio de Budapest)	**Artículo 224 ter. - Aseguramiento de Datos Informáticos almacenados**. Cuando existieren motivos para sospechar que los datos almacenados en un sistema informático dentro del territorio provincial pudieren ser alterados o suprimidos, el Fiscal podrá ordenar a cualquier persona humana o jurídica el aseguramiento de datos informáticos concretos y que estén a su disposición o para el que tiene legítimo acceso. Dicho aseguramiento podrá consistir en la conservación rápida de datos informáticos almacenados y la conservación y revelación parcial rápida de datos relativos al tráfico. La orden deberá especificar los datos concretos que se pretende conservar y la duración de la medida que no podrá exceder de noventa (90) días, por igual periodo si se mantuvieren los motivos que fundamentaron la orden.

Nº	Medidas de investigación	Medidas de investigación aprobadas por la Cámara de Senadores y Diputados de Mendoza (pendiente promulgación de Ejecutivo) + otras medidas ya reguladas en el CPP Mendoza
		La persona requerida deberá mantener en secreto la medida bajo apercibimiento de sanción penal.
2	Conservación y divulgación inmediata de los datos de tráfico (Artículo 17 Convenio de Budapest)	**Artículo 224 ter. - Aseguramiento de Datos Informáticos almacenados**. Cuando existieren motivos para sospechar que los datos almacenados en un sistema informático dentro del territorio provincial pudieren ser alterados o suprimidos, el Fiscal podrá ordenar a cualquier persona humana o jurídica el aseguramiento de datos informáticos concretos y que estén a su disposición o para el que tiene legítimo acceso. Dicho aseguramiento podrá consistir en la conservación rápida de datos informáticos almacenados y la conservación y revelación parcial rápida de datos relativos al tráfico. La orden deberá especificar los datos concretos que se pretende conservar y la duración de la medida que no podrá exceder de noventa (90) días, por igual periodo si se mantuvieren los motivos que fundamentaron la orden. La persona requerida deberá mantener en secreto la medida bajo apercibimiento de sanción penal.
3	Mandato de comunicación (Artículo 18 Convenio de Budapest)	**Artículo 224 bis. - Orden de Presentación de Datos Informáticos.** Siempre que se vincule con la investigación de un delito de su competencia, el Fiscal podrá ordenar por decreto fundado, a cualquier persona humana o jurídica en el territorio provincial, la presentación de datos informáticos, electrónicos o digitales o en un dispositivo de almacenamiento informático que obre en su poder o bajo su control, relativos a la identificación o localización u otra información asociada de un usuario y/o abonado, y que se pueda acceder al sistema legítimamente aunque no se encuentre dentro del territorio. Asimismo, el Fiscal podrá ordenar a toda persona humana o jurídica que preste un servicio de comunicaciones o a los proveedores de Internet de cualquier clase en jurisdicción argentina, la entrega de datos personales o de identificación de los usuarios y/o abonados u otra información asociada, que tengan bajo su poder o a los que pueda acceder de manera legítima, aunque estén fuera de esa jurisdicción. La orden podrá contener la indicación de que la medida deberá mantenerse secreta bajo apercibimiento de sanción penal y con las limitaciones establecidas en el Art. 225 del C.P.P. El destinatario quedará obligado a adoptar todas las medidas técnicas de seguridad necesarias, para mantener en secreto la medida ordenada por el Magistrado.
4	Registro y decomiso de datos informáticos almacenados (Artículo 19 Convenio de Budapest)	**Artículo 228 bis. - Secuestro, Apertura y Análisis de Sistema Informático e Incautación de Datos**. A pedido del Fiscal, el Juez Penal Colegiado podrá ordenar por decreto fundado, el registro de un sistema informático o de una parte de éste o de un medio de almacenamiento de datos informáticos o electrónicos, con el objeto de secuestrar los componentes del sistema, obtener copia o preservar datos o elementos de interés para la investigación, bajo las mismas condiciones establecidas en el Art. 216 del C.P.P. y con las limitaciones establecidas en el Art. 225 del C.P.P. La ejecución de la actuación se hará bajo la responsabilidad del Fiscal que

Nº	Medidas de investigación	Medidas de investigación aprobadas por la Cámara de Senadores y Diputados de Mendoza (pendiente promulgación de Ejecutivo) + otras medidas ya reguladas en el CPP Mendoza
		solicitó la medida. El Fiscal deberá indicar al juez: a) La individualización de los dispositivos o sistemas informáticos que serán objeto del registro, b) Una descripción del objeto concreto de la medida, c) La identificación de los mecanismos, metodología y herramientas mediante los cuales se almacenará la información obtenida que permitan asegurar la integridad de los datos y el resguardo de la cadena de custodia, d) El funcionario y/o quien designe como encargada de la ejecución del registro, copia o incautación de datos. Rigen en cuanto son aplicables todos los límites y garantías referidos al secuestro de cosas, documentos privados y correspondencia epistolar. En caso de que durante la ejecución de esta medida surjan elementos que permitan considerar que los datos buscados se encuentran almacenados en otro dispositivo o sistema conectado al inicial o estén disponibles para éste, dentro de la misma jurisdicción, quienes lleven adelante la medida podrán extenderla o ampliar el registro al otro sistema, previa comunicación con el agente Fiscal, quien deberá solicitar autorización telefónica del Juez Penal Colegiado competente. La mencionada comunicación no podrá ser delegada por el Fiscal de Instrucción a ningún funcionario judicial. El Juez, por decreto fundado deberá disponer la autorización o rechazo de la medida, notificándola por correo electrónico y/o en forma telefónica. En caso que la medida sea autorizada, el agente Fiscal deberá acompañar por escrito la solicitud fundada dentro de las 48 horas de realizada la medida. En caso de ser necesario, por la complejidad del asunto el Juez podrá librar la orden, consignando únicamente su parte dispositiva, difiriéndose los fundamentos de las mismas. Esta se efectuará, bajo pena de nulidad, en el plazo máximo de 24 horas a contar del momento de autorización de la orden. En los supuestos en que los datos se encuentren almacenados en otra jurisdicción, la medida de registro de datos podrá ampliarse a dispositivos o sistemas informáticos, solo en los siguientes supuestos: a) Cuando se obtenga el consentimiento voluntario y lícito de la persona con facultades para disponer de la revelación de los datos desde el dispositivo o sistema informático inicial al que se accedió legalmente. b) Cuando resulte posible recibir o acceder a los datos buscados desde el sistema original sin necesidad de realizar maniobras técnicas que signifiquen ejercer actos de poder jurisdiccional en otro Estado. c) Cuando por la estructura del sistema informático no resulte posible determinar en forma certera al momento de ejecución de la medida, la jurisdicción en la cual los datos están alojados físicamente y no resulte necesario para acceder a ellos de la realización de maniobras técnicas que signifiquen ejercer actos de poder jurisdiccional en otro Estado. En los supuestos b) y c) se procurará restringir lo máximo posible el alcance de la medida copiando los datos que resulten de interés para la investigación y sin la alteración, remoción o eliminación por cualquier forma de los datos a los que se accede. Una vez concluido el Proceso Penal, por sentencia firme, se dispondrá la

Nº	Medidas de investigación	Medidas de investigación aprobadas por la Cámara de Senadores y Diputados de Mendoza (pendiente promulgación de Ejecutivo) + otras medidas ya reguladas en el CPP Mendoza
		devolución de los dispositivos electrónicos secuestrados, que no fueren objeto de decomiso previa eliminación del material ilícito. Si en estricto cumplimiento de la ejecución de las medidas se encontraren de modo casual datos o archivos informáticos que evidencien la comisión de un delito distinto al que motivó la medida, se procederá a su secuestro y se comunicará al Fiscal interviniente
5	Recogida en tiempo real de datos de tráfico (Artículo 20 Convenio de Budapest)	**No se encontró medida especial aplicable.**
6	Interceptación de datos relativos al contenido (Artículo 21 Convenio de Budapest)	**Art. 227 - Intercepción de Correspondencia.** Siempre que lo considere útil para la averiguación de la verdad, el Tribunal podrá ordenar por decreto fundado, bajo pena de nulidad , la interceptación o el secuestro de la correspondencia postal, telegráfica, electrónica o de todo efecto remitido por el imputado o destinado al mismo, aunque sea bajo nombre supuesto. **Art. 229 - Intervención de Comunicaciones.** El Tribunal podrá ordenar por decreto fundado, bajo pena de nulidad, la intervención de las comunicaciones del imputado, cualquiera sea el medio técnico utilizado, para impedirlas o conocerlas. **Art. 229 bis.** Cuando se presuma la existencia de una Asociación Ilícita, en cualquier instancia y bajo cualquier régimen procesal, Leyes 1.908 y 6.730, el Juez de Garantías, previa evaluación del o los elementos indiciarios que justifiquen el pedido de intervención de las comunicaciones de los sospechosos, decretará fundada e inmediatamente la medida, disponiendo el tiempo de los mismos. **Art. 229 ter.** La intervención de las comunicaciones a las que se alude en los artículos precedentes, podrán extenderse hasta un plazo máximo de sesenta días, pudiendo ser prorrogado por igual término, si las circunstancias del caso lo requiere. No podrá concederse autorización para realizarla de manera indeterminada. Quedan prohibidas dentro de los procesos penales las intervenciones de las comunicaciones llevadas a cabo entre los imputados y sus abogados defensores. Vencidos los plazos establecidos el Juez dará vista al Ministerio Público para que determine la iniciación de la causa o su archivo. Si se ordenara el archivo, el Juez y Tribunal interviniente exclusiva y excluyentemente, será el ejecutor de la destrucción o borrado de los soportes de las grabaciones.
7	Agente encubierto digital	**Artículo 29 bis. - Agente encubierto digital.** En los casos de investigación de delitos en que resulte necesaria la intervención del agente en entornos o

Nº	Medidas de investigación	Medidas de investigación aprobadas por la Cámara de Senadores y Diputados de Mendoza (pendiente promulgación de Ejecutivo) + otras medidas ya reguladas en el CPP Mendoza
		plataformas digitales, el Fiscal podrá requerir fundadamente ante el Juez Penal Colegiado la actuación encubierta de un agente bajo las premisas anteriores y las condiciones aquí previstas. La autorización de este medio de investigación excepcional, se emitirá por decreto fundado, en el marco de la investigación de delitos previstos en los artículos 128, 131 del Código Penal, en delitos concretos de especial gravedad o de investigación compleja y siempre que existan motivos suficientes que acrediten: a) Que el éxito de la investigación esté seriamente dificultado de no recurrirse a este medio, b) Que se trata de delitos cometidos a través de medios informáticos que no permiten otra forma de investigación. La actuación encubierta no podrá exceder de ciento ochenta (180) días a contar desde que la autorización otorgada por el Juez Penal sea notificada al Fiscal. Los perfiles o identidades digitales, en ningún caso podrán ser imágenes de personas reales, serán creados y administrados por personal técnico idóneo del Ministerio Público Fiscal, funcionarios o auxiliares de la fuerza de seguridad en función judicial con experiencia y desarrollo en la materia, y bajo el control directo del Fiscal a cargo de la investigación, quien hará constar las directivas, reservando en caja de seguridad: la denominación y características del perfil utilizado por el agente encubierto; plataformas digitales donde se actuará; claves de acceso validadas y actividad concreta a desarrollar por el agente. Una vez concluida la intervención del agente encubierto digital, el Fiscal dejará constancias de su existencia en el legajo/expediente. El agente encubierto digital, con autorización específica para ello, podrá intercambiar o enviar por sí mismo archivos ilícitos por razón de su contenido. El agente encubierto informático estará exento de responsabilidad criminal por aquellas actuaciones que sean consecuencia necesaria del desarrollo de la investigación, siempre que guarden la debida proporcionalidad con la finalidad de ésta y no constituyan una provocación al delito. A los efectos del presente artículo se considera agente encubierto digital al funcionario de las fuerzas de seguridad o miembro del Ministerio Público Fiscal autorizado, que previo prestar su consentimiento, oculte o utilice un perfil digital encubierto, interactúe y se relacione digitalmente a través de tecnologías de la información y de la comunicación con el objeto de: identificar o detener a los autores, partícipes o encubridores de un delito; impedir la consumación de un delito; o para reunir información o elementos de prueba necesarios para la investigación.
8	Registro remoto	**No se encontró medida especial aplicable.**
9	OSINT	**No se encontró medida especial aplicable.**
10	Acceso transfronterizo de datos	**No se encontró medida especial aplicable.**
11	Hallazgos casuales	**No se encontró medida especial aplicable.**

Nº	Medidas de investigación	Medidas de investigación aprobadas por la Cámara de Senadores y Diputados de Mendoza (pendiente promulgación de Ejecutivo) + otras medidas ya reguladas en el CPP Mendoza
	en evidencia digital	
12	Desbloqueo compulsivo de datos informáticos	**No se encontró medida especial aplicable.**

Tabla Nº 27: Resumen de medidas de investigación reguladas en la Provincia de Mendoza (Argentina)

7.2.3.2. La figura del agente encubierto informático

Entre los aspectos más destacados de la normativa aprobada la Cámara de Senadores de Mendoza es la incorporación de la figura del Agente encubierto Informático, en los casos de la investigación de delitos en que resulte de utilidad la interacción del agente en entornos o plataformas digitales. Para ello el Agente Fiscal podrá requerir ante el Juez Penal Colegiado la actuación encubierta de un agente bajo las mismas premisas anteriores. La autorización de este medio de investigación excepcional, se emitirá -por decreto fundado-, en el marco de la investigación de un delito concreto de especial gravedad y siempre que existan motivos suficientes

Además se generará el Registro de un sistema informático e Incautación de datos. De esta manera, a pedido del Agente Fiscal, el Juez Penal Colegiado podrá ordenar por decreto fundado, el registro de un sistema informático o de una parte de este o de un medio de almacenamiento de datos informáticos o electrónicos, con el objeto de secuestrar los componentes del sistema, obtener copia o preservar datos o elementos de interés para la investigación, bajo las mismas condiciones establecidas en el Art. 216 del C.P.P. y con las limitaciones establecidas en el Art. 225 del C.P.P. La ejecución de la actuación se hará bajo la responsabilidad del Fiscal que solicitó la medida.

La propuesta además establece en cuanto a la limitación a la utilización de datos encontrados de forma casual, que cuando en el marco de la ejecución de la medida anterior, se hallaren datos o archivos informáticos que pueden resultar útiles

para la investigación de un hecho delictivo diferente al que motivó la autorización judicial, ellos solamente podrán ser incautados, previa autorización del Juez de Garantías actuante, cuando el Fiscal pueda acreditar que el hallazgo se produjo de manera casual mediante el uso normal del programa o mecanismo técnico utilizado, en el estricto cumplimiento de la búsqueda autorizada.

7.2.3.3. La orden aseguramiento y de presentación de datos

En cuanto al Orden de Presentación de Datos Informáticos, estipula que deberá realizarse siempre que se vincule con la investigación de un delito de su competencia. Para ello, el Agente Fiscal podrá ordenar por decreto fundado, a cualquier persona humana o jurídica en el territorio provincial, la presentación de datos informáticos, electrónicos o digitales o en un dispositivo de almacenamiento informático que obre en su poder o bajo su control, relativos a la identificación o localización de un usuario abonado y que se pueda acceder al sistema legítimamente aunque no se encuentre dentro del territorio.

Asimismo, el Fiscal de Instrucción podrá ordenar a toda persona humana o jurídica que preste un servicio de comunicaciones o a los proveedores de Internet de cualquier clase en jurisdicción argentina, la entrega de datos personales o de identificación de los usuarios y/o abonados, que tengan bajo su poder o a los que pueda acceder de manera legítima, aunque estén fuera de esa jurisdicción. La orden podrá contener la indicación de que la medida deberá mantenerse bajo secreto bajo apercibimiento de sanción penal. El destinatario quedará obligado a adoptar todas las medidas técnicas de seguridad necesarias, para mantener en secreto la medida ordenada por el Magistrado.

Además estipula en cuanto al aseguramiento de Datos Informáticos almacenados, que cuando existieren motivos para sospechar que los datos almacenados en un sistema informático dentro del territorio provincial pudieren ser alterados o suprimidos, el Fiscal de Instrucción podrá ordenar a cualquier persona física o jurídica el aseguramiento de datos informáticos concretos almacenados en un sistema informático que esté bajo su disposición o para el que tiene legítimo

acceso. Dicho aseguramiento podrá consistir en la conservación rápida de datos informáticos almacenados y la conservación y revelación parcial rápida de datos relativos al tráfico.

El proyecto impulsado por el Fiscal Sebastián Garay, también propuso modificaciones en cuanto a la custodia o depósito[512], que los efectos secuestrados serán inventariados y puestos bajo segura custodia a disposición del órgano judicial interviniente, o se ordenará su depósito. En el caso de los dispositivos electrónicos podrán ser solicitados en depósito al órgano judicial interviniente, por el Poder Ejecutivo -a través de funcionario que éste designe- para ser afectados exclusivamente al cumplimiento de la función de seguridad que compete a la Policía de la Provincia a través de la División Investigaciones o la que en su futuro la reemplace o por el Procurador General para ser destinados a la tarea de la Policía en función Judicial o a los Laboratorios Forenses.

Este artículo fue dejado fuera del cuadro, por considerar que en realidad no se trata de una medida o técnica especial de investigación , sino más bien de una medida procesal que apunta hacia la organización del proceso en sí, pero no sobre la propia investigación.

Por otro lado, también se regula que las cosas secuestradas serán aseguradas con faja de seguridad o mediante sistema de protección adecuado y sello del Tribunal o Fiscalía que intervenga, con la firma del Juez o Fiscal según corresponda y la firma del secretario, debiéndose firmar los documentos en cada una de sus hojas. Durante todo el procedimiento se deberán tomar las medidas necesarias y conducentes a fin de asegurar la cadena de custodia e integridad de las evidencias colectadas, dejando debido registro de todas las intervenciones realizadas sobre el material secuestrado.

---

[512] *Artículo 226.- Custodia o Depósito: Los efectos secuestrados serán inventariados y puestos bajo segura custodia a disposición del magistrado interviniente, o se ordenará su depósito. [...] Los dispositivos electrónicos podrán ser solicitados en depósito al magistrado interviniente, por el Poder Ejecutivo, a través de funcionario que éste designe, para ser afectados exclusivamente al cumplimiento de la función de seguridad que compete a la Policía de la Provincia a través de la División Investigaciones o la que en su futuro la reemplace o por el Procurador General para ser destinados a la tarea del Ministerio Público Fiscal o a los Laboratorios Forenses. Se podrá disponer la obtención de copias o reproducciones de las cosas secuestradas cuando éstas puedan desaparecer, alterarse, sean de difícil custodia o convenga así a la investigación penal preparatoria. [...]*

7.2.3.4. El registro remoto que no fue

Por último, comentar que quedó fuera del proyecto aprobado una propuesta inicial que formaba parte de la propuesta, donde consideraba también la incorporación de una medida de investigación que permitiera la realización de los registro o allanamiento remoto, bajo la siguiente propuesta:

> *Art. 3º: Incorpórese el artículo 216 ter: "Registro remoto de dispositivos tecnológicos que contengan evidencia digital". En supuestos urgentes, tratándose de delitos graves, previstos en los artículos 83, 140, 141, 142, 142 bis, 145, 145 bis, 145 ter, 146, 147 y 170 en el Título III del Código Penal de la Nación, cuando esté en riesgo la vida, la libertad o la integridad sexual de las personas, si hubiere motivos suficientes para presumir que en determinado dispositivo tecnológico o en un sistema informático, existe evidencia digital pertinente a la investigación delito, el Juez de Garantías interviniente, a solicitud del Fiscal de Instrucción, ordenará por decreto fundado, bajo pena de nulidad, el registro remoto de ese dispositivo mediante la instalación de un software que permita el examen a distancia de datos informáticos de existencia previa al registro, contenida en el dispositivo tecnológico. La orden debe ser escrita y fundada y deberá especificar: a) Los dispositivos tecnológicos objeto de la medida. b) El alcance de la misma y el software mediante el que se ejecutará el control de la información. c) Los agentes autorizados para la ejecución de la medida. d) Día y hora en que se realizará la medida e) Duración de la medida, que no podrá exceder de un plazo de 48 hs. Cuando quienes lleven a cabo el registro remoto, tengan motivos suficientes para considerar que los datos buscados están almacenados en otro sistema informático o en una parte del mismo, situado su territorio nacional, podrán ampliar el registro, siempre que los datos sean legítimamente accesibles por medio del sistema inicial o estén disponibles para este. Esta ampliación del registro deberá ser autorizada por el tribunal, salvo que ya lo hubiera sido en la autorización inicial".*

Como aspecto positivo para destacar, el proyecto mendocino identifica expresamente cuáles son los "*delitos graves*" del Código Penal que habilitan la realización de un registro remoto, como ser: "…supuestos urgentes, tratándose de delitos graves, previstos en los artículos 83, 140, 141, 142, 142 bis, 145, 145 bis, 145 ter, 146, 147 y 170 en el Título III del Código Penal de la Nación, cuando esté en riesgo la vida, la libertad o la integridad sexual de las personas".

Adicionalmente, destacamos la existencia del detalle sobre los fundamentos que debe contener el dictado de la medida, que permiten de alguna forma, un mayor nivel de garantías en la utilización de la misma.

Para no extendernos demasiado en esta subsección, y entendiendo que los comentarios aquí realizados pueden ser de utilidad para el lector por fuera de la

situación puntual de la Provincia de Mendoza, invitamos a ver mayor información en la sección de este mismo capítulo dedicada a técnicas especiales de investigación, específicamente el de registro remoto.

7.2.4. Neuquén

En el año 2014, la Provincia de Neuquén llevó adelante una profunda reforma procesal penal integral, con una importante cantidad de cambios, al punto tal que la Ley 2.784 (aprobada a finales de 2011 pero entró en vigencia en 2014).

Como se puede ver a continuación, entre esos cambios se introdujo puntualmente 2 artículos que en su extensión, logran regular, con mayor o menor detalle, gran parte de las medidas de investigación repasadas en este trabajo.

7.2.4.1. Cuadro de medidas de investigación reguladas

Nº	Medidas de investigación	Código Procesal Penal para la Provincia de Neuquén (Ley Nº 2784)
1	Conservación inmediata de datos informáticos almacenados (Artículo 16 Convenio de Budapest)	**Artículo 153º Información digital.** Cuando se hallaren dispositivos de almacenamiento de datos informáticos que por las circunstancias del caso hicieran presumir que contienen información útil a la investigación, se procederá a su secuestro, y de no ser posible, se obtendrá una copia. O podrá ordenarse la conservación de los datos contenidos en los mismos, por un plazo que no podrá superar los noventa (90) días. Quien deba cumplir esta orden deberá adoptar las medidas necesarias para mantenerla en secreto. También podrá disponerse el registro del dispositivo por medios técnicos y en forma remota. A cualquier persona física o jurídica que preste un servicio a distancia por vía electrónica, podrá requerírsele la entrega de la información que esté bajo su poder o control referida a los usuarios o abonados, o los datos de los mismos. La información que no resulte útil a la investigación, no podrá ser utilizada y deberá ser devuelta, previo ser puesta a disposición de la defensa, que podrá pedir su preservación. Regirán las limitaciones aplicables a los documentos.
2	Conservación y divulgación inmediata de los datos de tráfico (Artículo 17 Convenio de Budapest)	**Artículo 153º Información digital.** Cuando se hallaren dispositivos de almacenamiento de datos informáticos que por las circunstancias del caso hicieran presumir que contienen información útil a la investigación, se procederá a su secuestro, y de no ser posible, se obtendrá una copia. O podrá ordenarse la conservación de los datos contenidos en los mismos, por un plazo que no podrá superar los noventa (90) días. Quien deba cumplir esta orden deberá adoptar las medidas necesarias para

Nº	Medidas de investigación	Código Procesal Penal para la Provincia de Neuquén (Ley Nº 2784)
		mantenerla en secreto. También podrá disponerse el registro del dispositivo por medios técnicos y en forma remota. A cualquier persona física o jurídica que preste un servicio a distancia por vía electrónica, podrá requerírsele la entrega de la información que esté bajo su poder o control referida a los usuarios o abonados, o los datos de los mismos. La información que no resulte útil a la investigación, no podrá ser utilizada y deberá ser devuelta, previo ser puesta a disposición de la defensa, que podrá pedir su preservación. Regirán las limitaciones aplicables a los documentos.
3	Mandato de comunicación (Artículo 18 Convenio de Budapest)	**Artículo 153º Información digital.** Cuando se hallaren dispositivos de almacenamiento de datos informáticos que por las circunstancias del caso hicieran presumir que contienen información útil a la investigación, se procederá a su secuestro, y de no ser posible, se obtendrá una copia. O podrá ordenarse la conservación de los datos contenidos en los mismos, por un plazo que no podrá superar los noventa (90) días. Quien deba cumplir esta orden deberá adoptar las medidas necesarias para mantenerla en secreto. También podrá disponerse el registro del dispositivo por medios técnicos y en forma remota. A cualquier persona física o jurídica que preste un servicio a distancia por vía electrónica, podrá requerírsele la entrega de la información que esté bajo su poder o control referida a los usuarios o abonados, o los datos de los mismos. La información que no resulte útil a la investigación, no podrá ser utilizada y deberá ser devuelta, previo ser puesta a disposición de la defensa, que podrá pedir su preservación. Regirán las limitaciones aplicables a los documentos.
4	Registro y decomiso de datos informáticos almacenados (Artículo 19 Convenio de Budapest)	**Artículo 153º Información digital.** Cuando se hallaren dispositivos de almacenamiento de datos informáticos que por las circunstancias del caso hicieran presumir que contienen información útil a la investigación, se procederá a su secuestro, y de no ser posible, se obtendrá una copia. O podrá ordenarse la conservación de los datos contenidos en los mismos, por un plazo que no podrá superar los noventa (90) días. Quien deba cumplir esta orden deberá adoptar las medidas necesarias para mantenerla en secreto. También podrá disponerse el registro del dispositivo por medios técnicos y en forma remota. A cualquier persona física o jurídica que preste un servicio a distancia por vía electrónica, podrá requerírsele la entrega de la información que esté bajo su poder o control referida a los usuarios o abonados, o los datos de los mismos. La información que no resulte útil a la investigación, no podrá ser utilizada y deberá ser devuelta, previo ser puesta a disposición de la defensa, que podrá pedir su preservación. Regirán las limitaciones aplicables a los documentos.
5	Recogida en tiempo real de datos de tráfico (Artículo 20 Convenio de Budapest)	**Artículo 150º Comunicaciones.** Para el secuestro de correspondencia epistolar y para la interceptación por cualquier medio técnico de otras formas de comunicación personal, se requerirá autorización judicial y se procederá de modo análogo al allanamiento. Podrá ordenarse la obtención, aun en tiempo real, de los datos de tráfico de las comunicaciones transmitidas por un sistema informático y también el contenido de las mismas. La intervención de comunicaciones tendrá carácter excepcional y podrá

Nº	Medidas de investigación	Código Procesal Penal para la Provincia de Neuquén (Ley Nº 2784)
		renovarse cada quince (15) días, expresando los motivos que justifican la extensión del plazo. Las prórrogas no podrán superar los noventa (90) días.
6	Interceptación de datos relativos al contenido (Artículo 21 Convenio de Budapest)	**Artículo 150º Comunicaciones.** Para el secuestro de correspondencia epistolar y para la interceptación por cualquier medio técnico de otras formas de comunicación personal, se requerirá autorización judicial y se procederá de modo análogo al allanamiento. Podrá ordenarse la obtención, aun en tiempo real, de los datos de tráfico de las comunicaciones transmitidas por un sistema informático y también el contenido de las mismas. La intervención de comunicaciones tendrá carácter excepcional y podrá renovarse cada quince (15) días, expresando los motivos que justifican la extensión del plazo. Las prórrogas no podrán superar los noventa (90) días.
7	Agente encubierto digital	No se encontró
8	Registro remoto	**Artículo 153º Información digital.** Cuando se hallaren dispositivos de almacenamiento de datos informáticos que por las circunstancias del caso hicieran presumir que contienen información útil a la investigación, se procederá a su secuestro, y de no ser posible, se obtendrá una copia. O podrá ordenarse la conservación de los datos contenidos en los mismos, por un plazo que no podrá superar los noventa (90) días. Quien deba cumplir esta orden deberá adoptar las medidas necesarias para mantenerla en secreto. También podrá disponerse el registro del dispositivo por medios técnicos y en forma remota. A cualquier persona física o jurídica que preste un servicio a distancia por vía electrónica, podrá requerírsele la entrega de la información que esté bajo su poder o control referida a los usuarios o abonados, o los datos de los mismos. La información que no resulte útil a la investigación, no podrá ser utilizada y deberá ser devuelta, previo ser puesta a disposición de la defensa, que podrá pedir su preservación. Regirán las limitaciones aplicables a los documentos.
8	Registro remoto	**No se encontró medida especial aplicable.**
9	OSINT	**No se encontró medida especial aplicable.**
10	Acceso transfronterizo de datos	**No se encontró medida especial aplicable.**
11	Hallazgos casuales en evidencia digital	**No se encontró medida especial aplicable.**
12	Desbloqueo compulsivo de	**No se encontró medida especial aplicable.**

Nº	Medidas de investigación	Código Procesal Penal para la Provincia de Neuquén (Ley Nº 2784)
	datos informáticos	

Tabla Nº 28: Resumen de medidas de investigación reguladas en la Provincia de Mendoza (Argentina)

Dedicaremos algunos párrafos a realizar algunos comentarios al respecto de la regulación de Neuquén. En primer lugar, poner sobre la mesa una cuestión cronológica, señalando que su actualización procesal penal fue la primera en el país en incluir algún tipo de regulación sobre medidas de investigación relacionadas a la evidencia digital, a diferencia de las modificaciones realizadas en Mendoza y Salta, que son muchos más actuales (2023).

7.2.4.2. Conservación, decomiso y registro remoto

Abordando el texto de la modificación planteada por Neuquén, nos parece de interés comenzar por hacer algunos comentarios sobre el artículo 153 sobre información digital, artículo que de acuerdo a nuestro criterio, en mayor o menor medida, dispone regulación relacionada a: Conservación inmediata de datos informáticos almacenados; Conservación y divulgación inmediata de los datos de tráfico; Mandato de comunicación; Registro y decomiso de datos informáticos almacenados; y por último, sobre el tan polémico Registro Remoto.

Señalamos esto, para apuntalar nuestra primera crítica al respecto indicando que no consideramos adecuado, o al menos, no de una buena técnica legislativa, agrupar la regulación de tantas medidas diferentes dentro de un sólo artículo. Somos conscientes que al momento de proponer una reforma procesal penal (igual este no era el caso, toda vez que formó parte de una reforma integral desde cero), uno debe adaptarse al articulado ya existente. Sin embargo, es posible (como por ejemplo fue realizado en la Ley de Enjuiciamiento Criminal española), agregar incisos internos que permitan aportar a la prolijidad en la regulación.

Más allá del tema de la agrupación mencionada, es fácil advertir (a la luz de la regulación de las mismas medidas realizadas por otros países) la escasez de

regulación que permita limitar las medidas, que establezcan mayores detalles acerca de los requisitos para su aplicación, brindando mayor nivel de seguridad jurídica tanto para el fiscal que quiere solicitar la medida, el juez que debe autorizarla, así como para la propia defensa penal, en aras de la protección de los derechos y garantías de las personas investigadas.

En esta línea y sobre esta misma norma, el profesor y especialista Marcos Salt sostuvo una crítica afirmando que "*esta norma ya vigente no prevé un sistema de garantías adecuado para regular este mecanismo intrusivo. Del texto de la norma parece surgir que asimila los requisitos a los previstos para el allanamiento. Si bien habilita la medida legalmente bajo autorización judicial, la falta de claridad sobre los supuestos en los que puede ser aplicada y la posibilidad de afectación al principio de proporcionalidad ponen en duda su legitimidad constitucional*"[513].

Es interesante agregar que tampoco queda claro que tipo de registro remoto se ha querido regular aquí, porque por la escasa regulación proporcionada, podría tratarse de un intento de regulación para el registro remoto realizado en el marco de un allanamiento tradicional y no de un allanamiento remoto subrepticio (ver diferencias en la sección 6.3.3 de este trabajo).

7.2.4.3. Recolección de comunicaciones en tiempo real

Para dedicarle algunas líneas al otro artículo regulado (Art. 150 Comunicaciones) donde hemos considerado que su regulación podría considerarse que incluye tanto la medida de Recogida en tiempo real de datos de tráfico así como la Interceptación de datos relativos al contenido.

En este caso, se indica expresamente la posibilidad técnica de "*ordenarse la obtención, aun en tiempo real, de los datos de tráfico de las comunicaciones transmitidas por un sistema informático y también el contenido de las mismas".*

A diferencia del artículo anterior, aquí sí se han regulado algunos límites, como el hecho de mencionar que será una medida excepcional, que podrá ordenarse por

[513] SALT, Marcos; Tesis doctoral,, p. 98.

plazos de 15 días, justificando siempre la extensión del plazo. Por último, se dispone que las prórrogas no podrán superar los 90 días, estableciendo un límite a las mismas.

Como venimos afirmando reiteradamente a lo largo de esta tesis, celebramos siempre que en la regulación de medidas de investigación, el legislador se haya preocupado por establecer límites concretos que deban respetarse, al menos como principios al momento de ordenar las medidas. Entendemos que siempre existirán casos que por particularidades concretas, puedan necesitar moverse fuera de dichos límites, pero adherimos a la línea doctrinaria que entender que su inclusión, es la mejor decisión para la práctica de las investigaciones penales.

7.2.5. Salta

7.2.5.1. La generación de una Comisión Reformadora

En el año 2023 la Cámara de Senadores de la provincia norteña aprobó el proyecto de ley por el cual se reforma su código de forma incorporando procedimientos concretos para la investigación de delitos informáticos.

Lo hizo luego de obtener media sanción en la Cámara de Diputados y de que la Comisión de Legislación General, del Trabajo y Régimen Previsional de la provincia de Salta diera tratamiento al proyecto por el cual se modifican los artículos 309 y 316, incorporando los artículos 309 bis, 309 ter, 309 quater, 309 quinquies, 309 sexies, y 72 bis al Código Procesal Penal referente a la investigación penal en el ámbito digital, y aconsejara su sanción definitiva.

La reforma del Código Procesal Penal de Salta fue publicada en el Boletín Oficial de Salta como Ley n° 8386, que incorpora el tratamiento de evidencia digital e introduce modernas técnicas de investigación, es el trabajo final elaborado por la Comisión de Reforma dirigida por la Procuración General salteña.

La comisión fue integrada por el secretario de Justicia, Diego Sebastián Pérez; el director del Instituto de Derecho de las Telecomunicaciones, Informática y Nuevas

TICs del Colegio de Abogados y Procuradores, José Aráoz Fleming y representantes de universidades. Sofía Cornejo, actual fiscal de ciberdelincuencia, coordinó el equipo de trabajo, que fue asesorado por el director de la Carrera de Especialización en Cibercrimen y Evidencia Digital de la Facultad de Derecho de la Universidad de Buenos Aires, Marcos Salt[514].

A continuación realizaremos el relevamiento de lo regulado en la Provincia de Salta.

7.2.5.2. Cuadro de medidas de investigación reguladas

Nº	Medidas de investigación	Código Procesal Penal de Salta (Ley Nº 8386)
1	Conservación inmediata de datos informáticos almacenados (Artículo 16 Convenio de Budapest)	**Art. 309 bis.- Aseguramiento de datos.** El fiscal podrá ordenar a una persona física o jurídica el aseguramiento de datos informáticos concretos almacenados en un sistema informático o en un dispositivo de almacenamiento informático que esté bajo su disposición o control y para el que tenga legítimo acceso, cuando los datos puedan ser de utilidad en una investigación concreta y tenga motivos para sospechar que éstos pueden ser alterados o suprimidos o de cualquier forma dejar de estar disponibles. La orden deberá especificar los datos que se pretenden asegurar, la modalidad técnica de la conservación y la duración de la medida que no podrá exceder de noventa (90) días, prorrogables por igual período si se mantienen los motivos que fundamentaron la orden. El requerido deberá arbitrar los medios necesarios para preservar de inmediato la integridad de los datos en cuestión y, cuando así le sea ordenado, deberá mantener bajo secreto la medida de aseguramiento. Las personas involucradas en el cumplimiento de la orden deberán guardar reserva y abstenerse de informar sobre ellas en los términos del artículo 257 del presente Código. Cuando el objeto de la medida prevista en los párrafos anteriores sea el aseguramiento de datos de tráfico relativos a una determinada comunicación, el proveedor de servicio requerido informará al fiscal -lo antes posible- si hubiera otros proveedores de servicio por medio de los cuales aquella comunicación haya sido efectuada, con el fin de identificar a todos los proveedores de servicio intervinientes en la comunicación y que, de esa manera, se puedan arbitrar las medidas necesarias para asegurar los datos del tráfico de la comunicación.
2	Conservación y divulgación	**Art. 309 bis.- Aseguramiento de datos.** El fiscal podrá ordenar a una persona física o jurídica el aseguramiento de datos informáticos concretos almacenados en un sistema informático o en un dispositivo de almacenamiento informático

[514] DIARIO JUDICIAL, "Salta hackea las investigaciones"; Url: https://www.diariojudicial.com/news-95678-salta-hackea-las-investigaciones

Nº	Medidas de investigación	Código Procesal Penal de Salta (Ley Nº 8386)
	inmediata de los datos de tráfico (Artículo 17 Convenio de Budapest)	que esté bajo su disposición o control y para el que tenga legítimo acceso, cuando los datos puedan ser de utilidad en una investigación concreta y tenga motivos para sospechar que éstos pueden ser alterados o suprimidos o de cualquier forma dejar de estar disponibles. La orden deberá especificar los datos que se pretenden asegurar, la modalidad técnica de la conservación y la duración de la medida que no podrá exceder de noventa (90) días, prorrogables por igual período si se mantienen los motivos que fundamentaron la orden. El requerido deberá arbitrar los medios necesarios para preservar de inmediato la integridad de los datos en cuestión y, cuando así le sea ordenado, deberá mantener bajo secreto la medida de aseguramiento. Las personas involucradas en el cumplimiento de la orden deberán guardar reserva y abstenerse de informar sobre ellas en los términos del artículo 257 del presente Código. Cuando el objeto de la medida prevista en los párrafos anteriores sea el aseguramiento de datos de tráfico relativos a una determinada comunicación, el proveedor de servicio requerido informará al fiscal -lo antes posible- si hubiera otros proveedores de servicio por medio de los cuales aquella comunicación haya sido efectuada, con el fin de identificar a todos los proveedores de servicio intervinientes en la comunicación y que, de esa manera, se puedan arbitrar las medidas necesarias para asegurar los datos del tráfico de la comunicación.
3	Mandato de comunicación (Artículo 18 Convenio de Budapest)	**Art. 309 ter.- Orden de presentación de datos informáticos.** El Fiscal por sí o con autorización del Juez de Garantías, cuando por el tipo de dato solicitado se requiera orden judicial, podrá ordenar a todo organismo público y a cualquier persona física o jurídica en el territorio provincial que presente, remita o entregue datos alojados en un dispositivo de almacenamiento o sistema informático que esté bajo su poder o control y al que pueda acceder legítimamente, siempre que los datos solicitados se vinculen con la investigación de un delito concreto de su competencia. Asimismo, el fiscal, en el marco de una investigación penal concreta, podrá solicitar a toda persona física o jurídica con asiento fuera de la provincia de Salta (pero que preste un servicio de comunicaciones en ésta) o a los proveedores de servicios de Internet de cualquier tipo que allí brinden sus servicios, que presente, remita o entregue los datos de identificación de los usuarios y/o abonados, datos de conexión y los datos de facturación o pago con los que cuente en relación a dichos servicios, siempre que estén bajo su poder o control o a los que pueda acceder de manera legítima. La orden podrá contener la indicación de que la medida deberá mantenerse bajo secreto. Las personas involucradas en el cumplimiento de la orden deberán guardar reserva y abstenerse de informar sobre ellas en los términos del artículo 257 del presente y Código.
4	Registro y decomiso de datos informáticos almacenados	**Art. 309 quater.- Obtención de datos informáticos.** 1. Orden judicial. El Juez de Garantías podrá ordenar a requerimiento de parte y por auto fundado, el registro de un sistema informático o de una parte de éste, o de un medio de almacenamiento de datos informáticos o electrónicos, con el objeto de:

Nº	Medidas de investigación	Código Procesal Penal de Salta (Ley Nº 8386)
	(Artículo 19 Convenio de Budapest)	a) Secuestrar los componentes físicos del sistema y, si fuera necesario, los dispositivos para su lectura. En este supuesto regirán en cuanto sean aplicables, las previsiones del Capítulo V, procurando garantizar por medios físicos y técnicos la inalterabilidad de los datos contenidos en los soportes físicos secuestrados. b) Realizar copia en un soporte autónomo o en repositorio compartido de datos autorizado judicialmente, de todos los datos contenidos en los sistemas o dispositivos encontrados o de los datos que la orden judicial hubiera autorizado a secuestrar, garantizando por medios tecnológicos que los datos no puedan sufrir ningún tipo de modificación o alteración. c) Preservar por medios tecnológicos todos los datos contenidos en los dispositivos o aquellos datos identificados en la orden judicial asegurando que no puedan ser alterados o suprimidos. d) Remover o secuestrar los datos haciéndolos inaccesibles para terceros ajenos a las autoridades a cargo de la investigación. A los fines de una ejecución más eficiente de la orden, especialmente cuando se encuentren en el lugar en el que se ejecuta la medida múltiples dispositivos o un importante volumen de datos que dificulte la ejecución, el Juez de Garantías, a pedido del fiscal, podrá autorizar que se realicen en el lugar las operaciones de constatación técnica necesarias para determinar qué dispositivos informáticos o archivos pueden contener datos alcanzados por la orden judicial, con la finalidad de limitar la cantidad de dispositivos o datos a registrar, copiar o secuestrar. Estas operaciones técnicas también podrán ser autorizadas por el Juez de Garantías cuando exista urgencia para obtener datos determinados a fin de evitar la concreción de un peligro inmediato para la vida o integridad física de las personas. Se deberá garantizar con los medios tecnológicos disponibles que resulten adecuados, que estas operaciones técnicas sean auditables, a los fines de garantizar la cadena de custodia y la posibilidad de control posterior de la medida por parte de la defensa. Rige en cuanto sea aplicable lo dispuesto en el artículo 249. El Juez de Garantías podrá autorizar que durante la ejecución de una orden de obtención de datos se acceda en vivo a datos contenidos en memorias volátiles, cuando exista riesgo de alteración o pérdida. 2. Hallazgos casuales. Cuando en el marco de un registro de dispositivos o sistemas informáticos o durante las tareas de peritaje, las autoridades que ejecutan la medida adviertan la presencia de datos vinculados a un posible hecho ilícito diferente, deberán comunicarlo de inmediato al Juez de Garantías. Los datos así obtenidos sólo tendrán validez siempre y cuando hayan sido encontrados de manera casual en cumplimiento y siguiendo los parámetros y requisitos establecidos en la orden judicial original. 3. Extensión de registros. En los supuestos en los que durante la ejecución de una medida de obtención de datos de un sistema informático surjan elementos que permitan considerar que los datos buscados se encuentran almacenados en otro dispositivo o sistema informático, al que se tiene acceso lícito desde el dispositivo o sistema inicial, quienes llevan adelante la medida podrán extenderla al otro sistema. La ampliación del registro a los fines de la obtención o secuestro de datos deberá ser autorizada por el Juez de Garantías, quien fijará las condiciones de

Nº	Medidas de investigación	Código Procesal Penal de Salta (Ley Nº 8386)
		realización de la medida, salvo que esta situación estuviera prevista en la orden original. Cuando sea posible determinar que los datos que son objeto de la medida se encuentren almacenados en extraña jurisdicción, la obtención de datos solo podrá ampliarse: a) Si se cuenta con el consentimiento voluntario y lícito de la persona con facultades para disponer la revelación de los datos desde el dispositivo o sistema informático inicial. b) Cuando resulte posible recibir o acceder a los datos buscados desde el sistema original al que se accedió con la orden de obtención de datos, sin necesidad de realizar maniobras técnicas que signifiquen ejercer actos de poder jurisdiccional en extraña jurisdicción. c) Cuando no resulta posible determinar en forma certera, al momento de ejecución de la medida, la jurisdicción en la cual los datos están alojados. En los supuestos b) y c) se procurará restringir al máximo posible el alcance de la medida, copiando los datos que resulten de interés para la investigación y evitando la alteración, remoción o eliminación por cualquier forma de los datos a los que se accede. La obtención de datos en extraña jurisdicción se notificará al Juez de Garantías que ordenó la extensión de registro, quien evaluará la necesidad o conveniencia de informar la medida y sus resultados a las autoridades de la jurisdicción correspondiente, de acuerdo con las normas de cooperación judicial vigentes.
5	Recogida en tiempo real de datos de tráfico (Artículo 20 Convenio de Budapest)	**Art. 316.- Interceptación de correspondencia.** intervención de comunicaciones e interceptación de datos de tráfico y de contenido. El Juez de Garantías podrá ordenar, a pedido del Fiscal, cuando existan motivos que lo justifiquen y mediante auto fundado, las intervenciones de comunicaciones telefónicas y de cualquier otra comunicación a distancia, cursadas mediante otros medios, correspondientes al imputado o a quienes se comuniquen con él, para impedirlas o conocerlas. El auto que ordene la intervención en la comunicación deberá determinar los números telefónicos o precisar los medios a intervenir, las personas respecto de las cuales está dirigida, el objeto de la pesquisa y el tiempo por el cual se llevará a cabo. Asimismo, y bajo las mismas condiciones que para el caso anterior, se ordenará la intervención, a fin de interceptar datos de tráfico y contenido, los mensajes de correo electrónico que pertenezcan al imputado y/o sus comunicaciones on line, sean vía internet y/o intranet. El Juez de Garantías podrá autorizar el uso de los mecanismos tecnológicos previstos en el artículo 309 sexies, bajo las condiciones previstas en aquella norma. Si los elementos de convicción tenidos en consideración para ordenar la medida desaparecieren, hubiere transcurrido su plazo de duración, o alcanzado su objeto, ella deberá ser interrumpida inmediatamente. La intervención se ordenará por períodos de hasta treinta (30) días, los que podrán ser renovados mediante decreto fundado y cuando existan motivos que los justifiquen. El resultado de la medida se captará por medios técnicos que aseguren la

Nº	Medidas de investigación	Código Procesal Penal de Salta (Ley Nº 8386)
		fidelidad del registro y el Fiscal seleccionará las conversaciones vinculadas al objeto del proceso. El Fiscal y las partes deberán guardar secreto del contenido de la intervención. El Fiscal podrá disponer la transcripción de las partes pertinentes de la grabación, que se hará constar en un acta, sin perjuicio de conservar los originales. Queda terminantemente prohibida bajo sanción de nulidad, la intervención de teléfonos, correos electrónicos y/o las comunicaciones on line, sean vía internet y/o intranet de los abogados defensores y de los demás letrados con intervención en la causa. Igualmente, cualquier sistema de grabación que permita reproducir material propio del ejercicio de sus cargos. La infracción será considerada falta grave para quienes la ordenen, practiquen o consientan sin perjuicio de la responsabilidad penal que estos actos conlleven.
6	Interceptación de datos relativos al contenido (Artículo 21 Convenio de Budapest)	**Art. 316.- Interceptación de correspondencia.** intervención de comunicaciones e interceptación de datos de tráfico y de contenido. El Juez de Garantías podrá ordenar, a pedido del Fiscal, cuando existan motivos que lo justifiquen y mediante auto fundado, las intervenciones de comunicaciones telefónicas y de cualquier otra comunicación a distancia, cursadas mediante otros medios, correspondientes al imputado o a quienes se comuniquen con él, para impedirlas o conocerlas. El auto que ordene la intervención en la comunicación deberá determinar los números telefónicos o precisar los medios a intervenir, las personas respecto de las cuales está dirigida, el objeto de la pesquisa y el tiempo por el cual se llevará a cabo. Asimismo, y bajo las mismas condiciones que para el caso anterior, se ordenará la intervención, a fin de interceptar datos de tráfico y contenido, los mensajes de correo electrónico que pertenezcan al imputado y/o sus comunicaciones on line, sean vía internet y/o intranet. El Juez de Garantías podrá autorizar el uso de los mecanismos tecnológicos previstos en el artículo 309 sexies, bajo las condiciones previstas en aquella norma. Si los elementos de convicción tenidos en consideración para ordenar la medida desaparecieren, hubiere transcurrido su plazo de duración, o alcanzado su objeto, ella deberá ser interrumpida inmediatamente. La intervención se ordenará por períodos de hasta treinta (30) días, los que podrán ser renovados mediante decreto fundado y cuando existan motivos que los justifiquen. El resultado de la medida se captará por medios técnicos que aseguren la fidelidad del registro y el Fiscal seleccionará las conversaciones vinculadas al objeto del proceso. El Fiscal y las partes deberán guardar secreto del contenido de la intervención. El Fiscal podrá disponer la transcripción de las partes pertinentes de la grabación, que se hará constar en un acta, sin perjuicio de conservar los originales. Queda terminantemente prohibida bajo sanción de nulidad, la intervención de teléfonos, correos electrónicos y/o las comunicaciones on line, sean vía internet y/o intranet de los abogados defensores y de los demás letrados con

Nº	Medidas de investigación	Código Procesal Penal de Salta (Ley Nº 8386)
		intervención en la causa. Igualmente, cualquier sistema de grabación que permita reproducir material propio del ejercicio de sus cargos. La infracción será considerada falta grave para quienes la ordenen, practiquen o consientan sin perjuicio de la responsabilidad penal que estos actos conlleven.
7	Agente encubierto digital	**Art. 309 quinquies, - Investigación encubierta en entornos digitales.** El Juez de Garantías, a requerimiento de las partes, podrá autorizar en el marco de una investigación concreta en el que se investigue la comisión de delitos de especial gravedad, la realización de investigaciones encubiertas en medios de comunicación informáticas, redes sociales, sitios informáticos de venta e intercambio de archivos, productos o servicios, juegos en línea, sitios de comercio electrónico y cualquier otro sistema informático, con el fin de identificar o detener a los autores, partícipes o encubridores, impedir la consumación de un delito, o para reunir elementos de prueba útiles para la investigación. A tal fin, el Juez de Garantías podrá autorizar la designación de investigadores propuestos por el Ministerio Público Fiscal para que actúen en forma encubierta. Podrán ser agentes encubiertos digitales los integrantes de las fuerzas de seguridad y del Cuerpo de Investigaciones Fiscales. Los investigadores designados, podrán crear o utilizar perfiles o identidades digitales falsas poniendo en conocimiento al Fiscal a cargo de la investigación, quien deberá registrar toda la información necesaria respecto a los perfiles o identidades falsas, sistemas informáticos en los que se utilizarán, claves de acceso validadas y actividad concreta a desarrollar. El Juez de Garantías podrá autorizar que, durante la investigación encubierta, se intercambien archivos o contenidos ilícitos, se compren o vendan bienes, activos digitales o servicios, se participe de foros o grupos o cualquier actividad en entornos digitales dirigida a identificar a los responsables de los hechos ilícitos investigados. En estos supuestos, no serán punibles quienes, como consecuencia necesaria del desarrollo de la investigación encubierta encomendada, hubieran cometido un hecho ilícito, siempre que guarden la debida proporcionalidad con la finalidad de la investigación y no implique poner en peligro cierto la vida o la integridad psíquica o física de una persona o la imposición de un grave sufrimiento físico o moral a otro. La medida será autorizada por el plazo estrictamente necesario para lograr la individualización de los autores, partícipes o encubridores, o para obtener y asegurar los medios de prueba necesarios para su prosecución. La orden judicial que autorice la medida deberá fundamentar su necesidad, razonabilidad y proporcionalidad, justificando especialmente la ponderación de su utilidad con relación a la afectación de derechos fundamentales involucrados, la gravedad del hecho investigado y que no existen medios menos intrusivos de la intimidad del imputado que resulten útiles para alcanzar los mismos fines probatorios.
8	Registro remoto	**Art. 309 sexies.- Obtención remota de datos de dispositivos informáticos.** 1. Presupuestos. El Juez de Garantías podrá ordenar a pedido del fiscal, que la obtención de datos prevista en el artículo 309 quater se realice de forma remota y sin el conocimiento del titular o usuario del dispositivo o sistema que es objeto

Nº	Medidas de investigación	Código Procesal Penal de Salta (Ley Nº 8386)
		de investigación, mediante la utilización de programas informáticos u otros mecanismos tecnológicos, siempre que la orden se emita en el marco de la investigación de un delito concreto de especial gravedad y existan motivos suficientes que acrediten que los datos necesarios para la investigación no pueden ser obtenidos de una forma menos gravosa para los derechos del imputado, o que el éxito de la investigación esté seriamente dificultado sin recurrir a este medio de investigación excepcional. El Juez de Garantías podrá autorizar también esta medida, siempre justificando la proporcionalidad de la autorización, en aquellos casos en los que el delito se cometa a través de medios informáticos que tornen imposible otra forma de investigación. Cuando resulte necesario para la ejecución de la medida, a pedido del Fiscal, el Juez de Garantías podrá ordenar la colaboración de las empresas proveedoras de servicios de Internet o de comunicaciones o de terceras personas que tengan conocimientos especiales sobre las medidas de seguridad o el funcionamiento del sistema informático que es objeto de la medida. La orden no será aplicable a personas que puedan resultar imputadas o que estén alcanzadas por la dispensa de declarar como testigos por motivos de parentesco, amistad o estado. Rigen en cuanto son aplicables todos, los límites y garantías referidos al secuestro de cosas, documentos privados y correspondencia epistolar. 2. Orden judicial. La orden judicial deberá precisar: a) La individualización de los dispositivos o sistemas informáticos que serán objeto de la medida. b) Una descripción del objetivo concreto de la medida y los datos informáticos que se procura obtener. c) Fundamentación sobre la gravedad del delito y las razones tecnológicas que justifican la necesidad y proporcionalidad de la utilización. d) En la medida en que sea posible al momento de emitir la orden, los programas u otros mecanismos técnicos que se utilizaran para la ejecución. Si este dato se conociera con posterioridad deberá ser comunicado al Juez de Garantías de manera inmediata. e) La autoridad encargada de la ejecución. f) El plazo máximo autorizado para su ejecución procurando que la medida se realice en el menor tiempo posible, estimado en el caso concreto. 3. Límites. La utilización de estos mecanismos deberá limitarse estrictamente al objetivo y tiempo autorizado judicialmente. El Juez de Garantías deberá controlar periódicamente su ejecución y ordenar su cese apenas se cumplan con los objetivos de la orden, asegurando que se retiren del dispositivo o sistema cualquier programa o mecanismo tecnológico que se hubiera utilizado para su realización. No podrán ser incorporados al proceso datos obtenidos en exceso de la orden judicial que autorizó la medida. 4. Extensión. Cuando los agentes que lleven a cabo el registro remoto tengan razones para creer que los datos buscados están almacenados en otro sistema informático o en una parte de éste, pondrán este hecho en conocimiento del Fiscal quien solicitará al Juez de Garantías que autorice una ampliación de los

Nº	Medidas de investigación	Código Procesal Penal de Salta (Ley Nº 8386)
		términos del registro, conforme a lo previsto en el apartado 5 del presente artículo. 5. Comunicación. El Fiscal deberá poner en conocimiento la realización de la medida y sus resultados a la persona física o jurídica titular del dispositivo o sistema informático que haya sido objeto del acceso remoto y al imputado y su defensor, lo antes que resulte posible sin entorpecer los resultados de la investigación y siempre dentro de un plazo máximo de seis (6) meses desde su realización.
9	OSINT	**No se encontró medida especial aplicable.**
10	Acceso transfronterizo de datos	**Art. 309 quater.- Obtención de datos informáticos. [...]** 3. Extensión de registros. En los supuestos en los que durante la ejecución de una medida de obtención de datos de un sistema informático surjan elementos que permitan considerar que los datos buscados se encuentran almacenados en otro dispositivo o sistema informático, al que se tiene acceso lícito desde el dispositivo o sistema inicial, quienes llevan adelante la medida podrán extenderla al otro sistema. La ampliación del registro a los fines de la obtención o secuestro de datos deberá ser autorizada por el Juez de Garantías, quien fijará las condiciones de realización de la medida, salvo que esta situación estuviera prevista en la orden original. Cuando sea posible determinar que los datos que son objeto de la medida se encuentren almacenados en extraña jurisdicción, la obtención de datos solo podrá ampliarse: a) Si se cuenta con el consentimiento voluntario y lícito de la persona con facultades para disponer la revelación de los datos desde el dispositivo o sistema informático inicial. b) Cuando resulte posible recibir o acceder a los datos buscados desde el sistema original al que se accedió con la orden de obtención de datos, sin necesidad de realizar maniobras técnicas que signifiquen ejercer actos de poder jurisdiccional en extraña jurisdicción. c) Cuando no resulta posible determinar en forma certera, al momento de ejecución de la medida, la jurisdicción en la cual los datos están alojados. En los supuestos b) y c) se procurará restringir al máximo posible el alcance de la medida, copiando los datos que resulten de interés para la investigación y evitando la alteración, remoción o eliminación por cualquier forma de los datos a los que se accede. La obtención de datos en extraña jurisdicción se notificará al Juez de Garantías que ordenó la extensión de registro, quien evaluará la necesidad o conveniencia de informar la medida y sus resultados a las autoridades de la jurisdicción correspondiente, de acuerdo con las normas de cooperación judicial vigentes.
11	Hallazgos casuales en evidencia digital	**Art. 309 quater.- Obtención de datos informáticos.** [...] 2. Hallazgos casuales. Cuando en el marco de un registro de dispositivos o sistemas informáticos o durante las tareas de peritaje, las autoridades que ejecutan la medida adviertan la presencia de datos vinculados a un posible hecho ilícito diferente, deberán comunicarlo de inmediato al Juez de Garantías.

Nº	Medidas de investigación	Código Procesal Penal de Salta (Ley Nº 8386)
		Los datos así obtenidos sólo tendrán validez siempre y cuando hayan sido encontrados de manera casual en cumplimiento y siguiendo los parámetros y requisitos establecidos en la orden judicial original.
12	Desbloqueo compulsivo de datos informáticos	**No se encontró medida especial aplicable.**

Tabla Nº 29: Resumen de medidas de investigación reguladas en la Provincia de Mendoza (Argentina)

A continuación, realizaremos algunos comentarios breves de la regulación incorporada al Código Procesal Penal de Salta, que por el nivel de minuciosidad que la persona lectora habrá podido comprobar, sería tema suficiente para escribir un libro dedicado solamente a cubrir los pormenores jurídicos y procesales que trae como novedad esta reforma.

Como primer comentario, es celebrar que en Argentina, una de las Provincias haya decidido llevar a cabo una reforma con este nivel de rigurosidad procesal penal, teniendo tanta preocupación por evitar avances contra los derechos y garantías de las personas investigadas, que la propia reforma con el artículo 309[515] (que dado el cuadro comparativo que se busca realizar, ha quedado fuera del relevamiento formal), dedicado precisamente a tener en cuenta la aplicación de principios a las medidas de investigación.

Nos quedamos con la saludable redacción que se ha incorporado, afirmando que "*En el uso de estos medios de prueba se procurará siempre la menor afectación posible a los derechos de las personas investigadas conforme a las necesidades de la investigación. La resolución que la disponga o autorice deberá fundamentar la*

[515] "*Art. 309.- Medios de prueba informáticos. Principios generales. La realización de cualquiera de las medidas previstas en los artículos 309 bis, 309 ter, 309 quater, 309 quinquies y 309 sexies, deberá ser ordenada por el Juez de Garantías o, en los casos en los que no se requiere autorización judicial, podrá ser dispuesta por el fiscal, siempre en el marco de una investigación penal concreta, definiendo detalladamente el ámbito objetivo y subjetivo y la duración de la medida en virtud de su utilidad para la investigación.*
En el uso de estos medios de prueba se procurará siempre la menor afectación posible a los derechos de las personas investigadas conforme a las necesidades de la investigación.
La resolución que la disponga o autorice deberá fundamentar la idoneidad, necesidad y proporcionalidad de la medida de conformidad a lo previsto en el artículo 1° inciso c) del presente Código."

idoneidad, necesidad y proporcionalidad de la medida de conformidad a lo previsto en el artículo 1° inciso c) del presente Código."

De esta forma, tal como más adelante veremos que también se realiza en la Ley de Enjuiciamiento Criminal española, comienza dicha regulación afirmando los límites y principios que el Estado Provincial de Salta deberá tener siempre en consideración al momento de echar mano a la utilización de las medidas reguladas.

Dicho esto realizaremos algunos comentarios de los aspectos más sobresalientes -a nuestro entender- de la regulación de cada una de las medidas incorporadas.

Comenzando por el art. 309 bis sobre aseguramiento de datos, destacamos el detalle que se tuvo en cuenta con la previsión realizada cuando el aseguramiento de datos se encuentra dirigido hacia datos de tráfico relativos a una determinada comunicación, el ISP deberá informar al fiscal si observa que existen otros proveedores de servicios involucrados (con la finalidad de extender dicha orden a los otros ISP). Adicionalmente, tal como se recomienda en el Convenio de Budapest, se ha regulado la obligación de secreto que deberá conservarse por parte de las personas involucradas encargadas de asegurar los datos solicitados, con la finalidad de no frustrar los objetivos de la investigación en curso.

En relación a la regulación del art. 309 ter sobre orden de presunción de datos informáticos destacamos el detalle del final, afirmando que podrán pedirse "siempre que los datos solicitados se vinculen con la investigación de un delito concreto de su competencia". Si bien puede parecer una obviedad, siempre es importante destacar estos detalles para evitar la existencia de casos de utilización discrecional de recursos de investigación como ocurrió en la Provincia de Santa Fe[516].

En relación a la regulación del art. 309 quater sobre obtención de datos informáticos, celebramos el detalle en la descripción sobre las distintas formas autorizadas para el secuestro de datos, siendo de extrema utilidad en la práctica judicial a fin de diferenciar las opciones técnicas que podrían darse en un caso

[516] DIARIO EL LITORAL; "Los puntos más sorprendentes de la causa por espionaje ilegal"; Url: https://www.ellitoral.com/politica/marcelo-sain-colaboradores-imputados-causa-espionaje-sorpresas-santafe_0_MEBRtSElr4.html

determinado, sobre todo en los incisos a y b. A modo de comentario, afirmar que la opción del punto c[517] sobre la preservación de los datos recolectados, no debería ser una posibilidad sino una obligación para todos los casos, a fin de poder comprobar siempre la adecuada cadena de custodia de dichos datos. El último inciso d) que establece la posibilidad de remover o hacer inaccesibles (por ejemplo a través del cifrado) los datos para terceros ajenos a las autoridades a cargo de la investigación, entendemos que también será una opción a disposición de la fiscalía, que fundamente su necesidad para el caso concreto (por ejemplo, podría considerarse necesario en el caso de encontrar material de abuso sexual infantil).

En el segundo párrafo del mismo artículo, celebramos la excelente regulación sobre la posibilidad de realizar la técnica de "*triage*", ampliamente conocida en el mundo de la informática forense y que puede ser de extrema utilidad para casos que, como bien describe la normativa salteña, tengan una cantidad de dispositivos demasiado cuantiosa o bien, el volumen de datos sea demasiado grande (y que por lo tanto, obstaculice realizar una copia forense como autoriza el primer párrafo inc. b).

El *Triage* es un procedimiento que se toma prestado de la medicina, mediante el cual se evalúa rápidamente el estado de varios pacientes para establecer la prioridad y orden en que deben ser atendidos. En el ámbito de la informática forense, el triage es un análisis rápido que se realiza sobre un equipo para determinar si contiene evidencia o indicios que puedan ser de utilidad para una investigación. De esta forma se puede examinar rápidamente un conjunto de equipos y determinar su importancia para la investigación en curso[518].

El punto 2 del art. 309 quater aporta luz sobre otro de los grandes temas polémicos de la evidencia digital que es la de los hallazgos casuales. En este caso, se ha optado por la regulación de los casos donde dichos descubrimientos podrán ser válidos, siempre que hayan sido encontrados de manera casual en cumplimiento y siguiendo los parámetros y requisitos establecidos en la orden judicial original.

---

[517] "*c) Preservar por medios tecnológicos todos los datos contenidos en los dispositivos o aquellos datos identificados en la orden judicial asegurando que no puedan ser alterados o suprimidos.*"

[518] INFO-LAB; "Guía integral de empleo de la informática forense en el proceso penal"; Url: https://www.pensamientopenal.com.ar/system/files/2019/02/doctrina47360.pdf

Para esto, claro está, esa orden judicial original deberá tener el suficiente nivel de detalle a fin de evitar las tan utilizadas fórmulas judiciales que invitan en una pericia informática a traer al informe "*todo otro dato que sea considerado de interés para la causa*".

Para cerrar con el art. 309 quater, no podemos dejar de mencionar la regulación del párrafo tercero sobre la extensión de los registros, otro de los grandes temas debatidos en materia de evidencia digital. Es decir, es de importancia contar con esta regulación para supuestos "*en los que durante la ejecución de una medida de obtención de datos de un sistema informático surjan elementos que permitan considerar que los datos buscados se encuentran almacenados en otro dispositivo o sistema informático, al que se tiene acceso lícito desde el dispositivo o sistema inicial, quienes llevan adelante la medida podrán extenderla al otro sistema"*. Destacamos en este punto el requisito que el acceso a ese "otro sistema" interconectado debe ser "lícito".

Entendemos que la regulación de estos casos habilitaría la posibilidad jurídica para poder legitimar aquellos accesos donde al momento de la requisa de un sistema, el o la especialista determinar que existen otros sistemas interconectados (por ejemplo un repositorio de un servidor que se encuentre en Telecom o Claro) que podrían (en potencial aún) contener la información de interés que se está buscando. se encuentre vinculado al equipo que está siendo requisado. Por el contrario, en el caso del desbaratamiento de una banda de cibercrimen dedicada al ransomware, si se tuviera la oportunidad de acceder a equipos encendidos con diversas conexiones a otros sistemas interconectados de empresas víctimas, su acceso no estaría habilitado toda vez que el mismo no sería lícito (entendiendo que los propietarios de dichos sistemas nunca han dado sus respectivos consentimientos).

Como advertimos anteriormente, no pretendemos aquí hacer un abordaje completo sobre todo lo interesante que podríamos señalar de la incorporación normativa de la Provincia de Salta, por lo que invitamos a la persona lectora, y desde ya consideramos que el análisis profundo y pormenorizado de la normativa salteña es una de las deudas pendientes y líneas de investigación que a futuro dejamos la posibilidad de continuar investigando.

No obstante, consideramos de relevancia realizar dos breves consideraciones extras acerca de las dos figuras más novedosas en materia de investigación de cibercrimen, que son la figura del agente encubierto digital y el registro remoto.

7.2.5.3. La inclusión del Agente encubierto digital

Nos ahorraremos toda la introducción y aspectos generales de la figura, para la cuál remitimos a la sección 6.3.2 de este mismo capítulo y avanzaremos con algunos comentarios particulares relacionados a la elección normativa de Salta.

El art. 309 quinquies habilita la utilización de la figura (autorizada por Juez de Garantías) para casos de delitos de "especial gravedad", sin quedar con demasiada claridad cuáles son estos delitos. La no restricción del instituto a la investigación de determinados delitos (como pasa con la figura tradicional del agente encubierto en la Ley Nº 27319). Entendemos que aquí se ha optado por dejar al criterio jurisdiccional salteño, la decisión si la causa investigada reviste o no esta especial gravedad.

Luego se realiza una enunciación acerca de los distintos espacios que podrían ser abordados por la figura (redes sociales, sitios de intercambio de archivos, etc.) y finaliza con "y cualquier otro sistema informático", que en definitiva, es el concepto más genérico de todos. Al finalizar el primer párrafo, describe que el instituto podrá ser utilizado para distintos fines, coincidiendo con los regulados en el art. 2 de la Ley Nº 27319.

Otro detalle es que, nada se dice acerca de que al momento de la aprobación de la medida de investigación por parte del Juez de Garantías, la resolución por la que se acuerde no necesita obligatoriamente consignar el nombre verdadero del agente y la identidad supuesta con la que actuará en el caso concreto (como por ejemplo se exige en la normativa española).

Destacamos que en el 4to párrafo del art. 309 quinquies, se ha dedicado unas líneas a la posibilidad cierta de que el agente encubierto digital, en el marco de sus maniobras para ingresar o permanecer en un grupo delictivo a fines de conseguir información útil a la investigación, pueda estar autorizado para el intercambio de

archivos o contenidos ilícitos (algo muy común en los grupos donde se comparte material de abuso sexual infantil), así como a comprar o vender activos o servicios. Consideramos de relevancia la incorporación de esta posibilidad, toda vez que la existencia de la figura del agente encubierto digital, sin esta posibilidad, puede en algunos casos, tornarse inútil a los fines buscados.

Para cerrar con esta figura, destacamos que en el último párrafo se hace una nueva referencia a que dicha medida deberá ser fundada en su necesidad, razonabilidad y proporcionalidad, justificando que no existan medios menos intrusivos de la intimidad del imputado (y de terceros que puedan estar ajenos a la investigación principal) que resulten útiles a la investigación. Nuevamente reforzando esta mirada del cuidado a los derechos y garantías que se ha tenido en cuenta en la reforma salteña, que como bien hemos señalado, en el primer artículo que se ha incorporado (art. 309) se ha realizado un buen trabajo preventivo que busque evitar o al menos minimizar la discrecionalidad o el abuso de estas figuras especiales de investigación.

7.2.5.4. Obtención remota de datos de dispositivos informáticos

Hacemos referencias a los aspectos genéricos de esta medida de investigación, que ya han sido abordados en la sección 6.3.3 de este mismo capítulo y avanzaremos con algunos comentarios particulares relacionados a la elección normativa de Salta.

Nos parece adecuado comenzar destacando que al comenzar el artículo se hace referencia a que esta figura es una forma alternativa o diferente de la figura del art. 309 quater, es decir, de la medida de obtención de datos informáticos, que a diferencia de la figura tradicional, será realizado de forma remota y sin el consentimiento del titular o usuario del dispositivo o sistema objeto de la medida. Sobre este punto, hacemos referencia a la teoría ya desarrollada, diferenciando el registro remoto con o sin consentimiento del titular desarrollado en la sección 6.3.3.1 y 2.

En el mismo párrafo, se destaca que este acceso remoto sin consentimiento del titular será realizado "*mediante la utilización de programas informáticos u otros mecanismos tecnológicos, siempre que la orden se emita en el marco de la investigación de un delito concreto de especial gravedad y existan motivos suficientes que acrediten que los datos necesarios para la investigación no pueden ser obtenidos de una forma menos gravosa para los derechos del imputado, o que el éxito de la investigación esté seriamente dificultado sin recurrir a este medio de investigación excepcional.*". Sobre el final volvemos a encontrar la misma fórmula que ya hemos celebrado en la figura del agente encubierto digital, por lo haremos referencia a lo ya dicho en el punto anterior.

Nos interesa destacar el hecho que se ha regulado que el acceso remoto podrá ser a través de la utilización de programas informáticos u otros mecanismos tecnológicos, toda vez que podría darse por ejemplo, la utilización de drones u otros dispositivos que, a partir de técnicas de conexión a redes o sistemas informáticos, podrían infiltrarse y obtener información de interés para la causa. Entendemos que otro mecanismo tecnológico que podría ser utilizado, sería algún dispositivo de hardware (keylogger por ejemplo) que tiene que conectarse en el equipo de la persona investigada, o al menos, dejarse físicamente en algún lugar cercano para lograr interceptar y periódicamente dicho dispositivo va registrando todas las teclas empleadas y enviandolas a una casilla de correo que se defina previamente.

Continuando con el análisis de la medida, se establece que cuando resulte necesario para la ejecución de la medida, "*a pedido del Fiscal, el Juez de Garantías podrá ordenar la colaboración de las empresas proveedoras de servicios de Internet o de comunicaciones o de terceras personas que tengan conocimientos especiales sobre las medidas de seguridad o el funcionamiento del sistema informático que es objeto de la medida*".

Sobre este aspecto, inicialmente entendíamos el pedido de colaboración a *terceras personas que tengan conocimientos especiales sobre las medidas de seguridad o el funcionamiento del sistema informático que es objeto de la medida*, se ha pensado con la finalidad de poder contar con la cooperación de administradores de sistemas de una empresa, que por ejemplo, puedan facilitar los accesos o

permisos para que los especialistas forenses puedan acceder a los sistemas. Sin embargo, eso podría ser útil para el caso de que el acceso sea con conocimiento del titular del sistema (por ejemplo una empresa), pero no es el caso, toda vez que esta medida ha sido pensada para acceder a un sistema informático de forma subrepticia. Entendemos entonces que aquí la norma habilitaría por ejemplo, a solicitar cooperación de un hacker que tenga profundos conocimientos sobre un sistema determinado, que brinde sus conocimientos para facilitar la ejecución de esta medida de investigación. Si es así, nos preguntamos, ¿sería a título gratuito? ¿podría negarse a cooperar? ¿Si se negara, tendría consecuencias penales? No pretendemos aquí dar ningún tipo de respuesta al respecto,de un tema que, como hemos adelantado, excede con creces el objeto concreto de este estudio.

En el punto 2, se detalla 6 elementos que deberán ser definidos en la propia orden judicial que autorice la medida, donde encontramos desde la individualización del dispositivo o sistema objeto del ingreso (por ejemplo, una notebook MacBook Pro), el objetivo o datos concretos que se esperan obtener (evidencia que lo vincule con un caso de grooming), fundamentación sobre la gravedad del delito y las razones tecnológicas que justifican su necesidad.

Nos detenemos aquí, no para hablar sobre la gravedad del delito, algo sobre lo que ya nos hemos expresado anteriormente, sino por el hecho que en la fundamentación, sea necesario explicar las razones tecnológicas que justifican la medida, algo que nos parece de notable importancia. En un contexto actual, donde los ciberdelincuentes más precavidos suelen adoptar diferentes técnicas antiforenses o antirastreo (que ya hemos desarrollado anteriormente, pero que un ejemplo sería cifrar sus dispositivos), aún sabiendo donde se encuentre y teniendo la posibilidad de realizar un allanamiento tradicional, se corre el riesgo de no conseguir la evidencia necesaria para avanzar en la imputación buscada. Otro caso, sería en aquellos donde, por ejemplo, porque utiliza alguna VPN para ocultar el verdadero origen de su conexión. En estos casos, acceder subrepticiamente al sistema, podría brindar la información necesaria para poder identificar al cibercriminal.

Continuando con el resto de los requerimientos que deben estar en la orden judicial, el punto d) menciona los programas o mecanismos técnicos que serán

utilizados, dejando la posibilidad que, en el caso que no se tenga certeza, podrán ser comunicados con posterioridad al Juez de Garantías. Desde nuestro conocimiento técnico, entendemos que es muy posible que esto pase mucho más de lo esperado, toda vez que saber con anticipación el programa o sistema a utilizar para el caso concreto, es muy complejo, toda vez que dependerá de una gran cantidad de detalles técnicos concretos (como sistema operativo, versión, tipo de conexión, que tipo de protección de seguridad posee el sistema, entre otros aspectos). Por último, señalar que la orden deberá contener la autoridad encargada de la ejecución (entendemos que será alguna fuerza de seguridad que posea este tipo de tecnologías que permita alguna posibilidad de éxito), y el plazo máximo autorizado para la ejecución de la misma.

7.2.5.5. La novedad en el Acceso a datos almacenados en extraña jurisdicción

Para ir cerrando con esta Provincia, señalamos la interesante incorporación de la parte final del art. 309 quater, relacionado a casos cuando sea posible determinar que los datos que son objeto de la medida se encuentren almacenados en extraña jurisdicción. Ante estos casos, la norma establece que la obtención de datos solo podrá ampliarse cuando:

> *a) Si se cuenta con el consentimiento voluntario y lícito de la persona con facultades para disponer la revelación de los datos desde el dispositivo o sistema informático inicial.*
>
> *b) Cuando resulte posible recibir o acceder a los datos buscados desde el sistema original al que se accedió con la orden de obtención de datos, sin necesidad de realizar maniobras técnicas que signifiquen ejercer actos de poder jurisdiccional en extraña jurisdicción.*
>
> *c) Cuando no resulta posible determinar en forma certera, al momento de ejecución de la medida, la jurisdicción en la cual los datos están alojados.*

De estas opciones, destacamos que el inciso a, sería una de las causales habilitantes de acuerdo al art. 32 de la Convención de Budapest, donde se regula el tema del acceso transfronterizo de datos.

Sin embargo, la novedad -a nuestro humilde criterio- es la regulación de los incisos b y c, que permitiría que dicho acceso transfronterizo para el acceso de datos se realice *"siempre que no sea necesario realizar maniobras técnicas que signifiquen ejercer actos de poder jurisdiccional en extraña jurisdicción*". La regulación no podría ser más precisa, toda vez que es exactamente eso lo que potencialmente podría cuestionar la defensa en el caso de un acceso. Entendemos que por ejemplo, si el sistema ya posee sus credenciales logueadas (por ejemplo en el caso de Google Drive), sería un caso donde perfectamente podría considerarse la aplicación de este inciso, toda vez que claramente la información a la que estamos accediendo no está en Argentina, pero en su acceso, no se estaría "forzando" ninguna puerta, permitiendo un acceso limpio a los sistemas. La clave estará entonces en las maniobras técnicas implementadas para el acceso a esos sistemas interconectados. Si por el contrario, dichos sistemas tuvieran restricciones de accesos, cuya contraseña fuera descubierta a través de un ataque de fuerza bruta, podríamos llegar a considerar que sería un caso donde habría un acto de poder jurisdiccional en extraña jurisdicción.

Por último, es muy novedosa la incorporación del caso del inc. c) donde se ha dejado una puerta abierta para aquellos casos donde no sea posible, al momento de ejecución de la medida, la determinación de la jurisdicción en la cuál están alojados los mismos. No nos queda claro si esta duda implica en la determinación de entre un país u otro (por ejemplo, si la información de Dropbox está en Irlanda o en EEUU) o si bien, esa duda implica si se encuentra en territorio nacional o internacional. No obstante, entendemos que esta regla puede ser importante para las investigaciones, a fin de que, en caso de dudas (es decir, cuando no sea técnicamente posible saber dónde se encuentran realmente los datos), se tenga una presunción a favor de la legitimidad de su acceso y de su incorporación a la investigación en curso.

7.3. Medidas de investigación reguladas en Brasil

7.3.1. El marco civil de internet y su importancia en la investigación

Consideramos de interés remarcar que en fecha 8 de julio de 2013, tras darse a conocer el espionaje del que la presidenta Dilma Rousseff era objeto por parte del gobierno de Estados Unidos a través de la Agencia Nacional de Inteligencia (NSA)[519], se urgió por a aprobación del Marco Civil para garantizar los derechos digitales de los ciudadanos y la soberanía tecnológica brasileña[520].

Vale decir que el texto de esta normativa del Marco Civil de Internet no fue creado de la noche a la mañana, sino que de hecho fue la primera legislación creada a través de procesos en línea (crowdsourcing) de Brasil, elaborada en 2009 de manera colaborativa, por una iniciativa entre la Secretaría de Asuntos Legislativos del Ministerio de Justicia (SAL-MJ) y la Escuela de Derecho de la Fundación Getúlio Vargas de Río de Janeiro (FGV-Rio), utilizando la plataforma culturadigital.br. La elaboración inicial tuvo dos fases: la primera fase permitió que cualquier ciudadano o institución comente los principios referentes al uso de Internet inspirado en los "Principios para la Gobernanza y Uso de Internet en Brasil" del Comité Gestor de Internet en Brasil (CGI.br)[521].

A continuación, se elaboró un texto de una ley basada en los inputs recibidos y fue puesto a disposición en una plataforma donde los ciudadanos podían comentar los artículos individuales. Durante las dos fases, el equipo responsable también recogió contribuciones en los foros de discusión y en Twitter a través del hashtag #marcocivil y del usuario @marcocivil. En 2011, el proyecto de ley fue enviado al Congreso Nacional y recibió otra ronda de discusiones abiertas iniciadas por el

[519] EL ECONOMISTA; "Denuncian a Enrique Peña Nieto por espionaje"; Disponible en: "https://www.eleconomista.com.mx/politica/Denuncian-a-Enrique-Pena-Nieto-por-espionaje-20170627-0040.html"

[520] AGENCIA BRASIL; "Tras las acusaciones de espionaje, el Gobierno pedirá celeridad en la votación del Marco de Derechos Civiles en Internet"; Disponible en: https://memoria.ebc.com.br/agenciabrasil/noticia/2013-07-08/apos-denuncias-de-espionagem-governo-pedira-agilidade-na-votacao-do-marco-civil-da-internet

[521] POGREBINSCHI, Thamy. (2017). LATINNO Dataset. Berlin: WZB.

relator en la Cámara de Diputados, el Diputado Alessandro Molon, en la Plataforma e-Democracia (hoy conocida como Wikilegis).

Sólo en 2014 se aprobó el proyecto que se convirtió en la Ley Federal Nº. 12.965/2014. Aunque las posteriores iniciativas legislativas que se utilizaron de métodos colaborativos en línea recibieron un mayor número de insumos y participación, Marco Civil de Internet fue una iniciativa innovadora, ya que es conocido en todo el mundo por ser la primera Declaración de Derechos de Internet, legislando sobre derechos digitales innovadores, como la neutralidad de la red y el establecimiento del multisectorialismo como principio para futuras regulaciones de internet en el país.

La metodología para la creación de una ley para Internet, en Internet, es decir, abierta y en colaboración, ha sido reconocida por actores políticos, gestores públicos y, en particular, por Sir Tim Berners-Lee, el creador de la World Wide Web.

La iniciativa, bautizada con el epíteto de Constitución de Internet, como se indica en la enmienda, "*establece los principios, garantías, derechos y deberes para el uso de Internet en Brasil*". Además de ser una declaración de principios para los usuarios y garantizar la privacidad, los derechos humanos y el ejercicio de la ciudadanía en los medios digitales, la propuesta también trató de regular diversos aspectos relacionados con la explotación comercial y gubernamental de la gran red. Ha habido muchas controversias en los temas abordados. La custodia de los datos de los usuarios por parte de las empresas de conexión con la internet y de las empresas responsables de los contenidos disponibles en Internet, la neutralidad de la red y el almacenamiento de los datos de usuarios de Internet en el país estaban entre los temas que han generado más enfrentamientos entre las empresas de telecomunicaciones y de contenido en Internet, los titulares de derechos de autor, el gobierno, grupos articulados de usuarios y muchos más[522].

[522] CÁMARA DE DIPUTADOS DE BRASIL, Libro "Marco Civil Brasileño de Internet en Español", 2015, Disponible en: https://eva.fing.edu.uy/pluginfile.php/99128/mod_resource/content/1/marco_%20civil%20_internet.pdf

7.3.2. La situación de Brasil según la ONU

En un estudio realizado en 2019 por Naciones Unidas en relación a la situación en relación al delito cibernético[523], en el considerando 52, Brasil informó que *"La amplitud geográfica de esos delitos informáticos había desafiado también los mecanismos tradicionales mediante los cuales el Brasil brindaba y recibía cooperación jurídica internacional. Los desafíos eran enormes: los proveedores de servicios de Internet, que poseían la información necesaria para investigar la ciberdelincuencia y reunir pruebas electrónicas, a menudo tenían su sede física en un país, prestaban servicios en distintos continentes y almacenaban su información en servidores localizados en cualquier otra parte del planeta. En ese contexto, los agentes de las fuerzas del orden se esforzaban por determinar quién tenía competencia sobre los datos y acceso directo a ellos y dirigirse debidamente a esa persona. Las solicitudes de cooperación internacional, a menudo canalizadas a través de tratados de asistencia judicial recíproca, se tramitaban muy lentamente y a veces quedaban privadas de efecto, dado el ritmo al que se eliminaban los datos digitales."*

Adicionalmente en el mismo estudio, Brasil informó de que, cada vez que había un elemento internacional en las investigaciones y en la jurisdicción, el desarrollo jurídico de un caso solía ralentizarse debido a las divergencias con respecto al significado de la protección de la privacidad, conforme quedaba reflejado en los diversos requisitos nacionales en materia de divulgación de datos. Otra dificultad para la cooperación jurídica internacional era la extrema volatilidad de las pruebas digitales, puesto que la enorme cantidad de información que circulaba por todo el mundo y los costos de almacenamiento hacían que las empresas no conservaran los datos durante más tiempo del estrictamente necesario para sus negocios[524].

[523] NACIONES UNIDAS, Asamblea General, "Lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos", 2019, Disponible en: https://www.unodc.org/documents/Cybercrime/SG_report/V1908185_S.pdf

[524] NACIONES UNIDAS, Asamblea General, "Lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos", 2019, Disponible en: https://www.unodc.org/documents/Cybercrime/SG_report/V1908185_S.pdf

7.3.3. Cuadro de medidas de investigación reguladas

Nº	Medidas de investigación	Regulación de medidas de investigación en Brasil
1	Conservación inmediata de datos informáticos almacenados (Artículo 16 Convenio de Budapest)	**Ley Nº 12.965/2014 - Marco Civil de Internet - Subsección I De la Custodia de Registros de Conexión Artículo 13.** En la provisión de conexión a Internet, cabe al administrador del sistema autónomo respectivo el deber de mantener los registros de conexión, bajo secreto, en un ambiente controlado y seguro, durante el plazo de un año, según el reglamento. § 1º La responsabilidad de mantener los registros de conexión no puede ser transferida a terceros. § 2º La autoridad policial o administrativa o el Ministerio Público podrá requerir cautelarmente que los registros de conexión sean guardados durante un plazo superior al previsto en este artículo. § 3º En la hipótesis del § 2º, la autoridad solicitante tendrá el plazo de sesenta días, contados a partir de la solicitud, para ingresar, con el pedido de autorización judicial, a los registros previstos en este artículo. § 4º El proveedor responsable de la custodia de los registros deberá mantener el secreto en relación a la solicitud prevista en el § 2º, que perderá su eficacia en caso de que el pedido de autorización judicial no sea aceptado o no haya sido ejecutado en el plazo previsto en el § 3º. § 5º En cualquier caso, la disponibilidad al requirente de los registros de los que trata este artículo deberá ser precedida de una autorización judicial, conforme a lo dispuesto en la Sección IV de este capítulo. § 6º En la aplicación de sanciones por el incumplimiento de lo dispuesto en este artículo, serán considerados la naturaleza, la gravedad de la infracción y los daños resultantes de ella, eventual beneficio para el infractor, las circunstancias agravantes, los antecedentes del infractor y la reincidencia. **Subsección III De la Custodia de Registros de Acceso a Aplicaciones de Internet en la Provisión de Aplicaciones Artículo 15**. El proveedor de aplicaciones de Internet constituido en forma de persona jurídica, que ejerza esa actividad en forma organizada, profesionalmente y con fines económicos, deberá mantener los respectivos registros de acceso a aplicaciones de Internet, en secreto, en ambiente controlado y de seguridad, por el plazo de seis meses, en los términos del reglamento. § 1º Orden judicial podrá obligar, por tiempo determinado, a los proveedores de aplicaciones de Internet, que no estén sujetos a lo dispuesto en el artículo a guardar registros de acceso a aplicaciones de Internet, si se tratan de registros relativos a hechos específicos en un tiempo determinado. § 2º La autoridad policial o administrativa o el Ministerio Público podrán solicitar cautelarmente a cualquier proveedor de aplicaciones de Internet que los registros de acceso a aplicaciones de Internet sean guardados, incluso por plazo superior al previsto en el artículo, observando lo dispuesto en los §§ 3º y 4º del artículo 13. § 3º En cualquier caso, la disponibilidad al requirente, de los registros de los que trata este artículo, deberá ser precedida de autorización judicial, conforme lo dispuesto en la Sección IV de este Capítulo. § 4º En la aplicación de sanciones por el incumplimiento de lo dispuesto en este

Nº	Medidas de investigación	Regulación de medidas de investigación en Brasil
		artículo, serán considerados la naturaleza y gravedad de la infracción, los daños resultantes de ella, el eventual beneficio para el infractor, las circunstancias agravantes, los antecedentes del infractor y la reincidencia.
2	Conservación y divulgación inmediata de los datos de tráfico (Artículo 17 Convenio de Budapest)	**Ley Nº 12.965/2014 - Marco Civil de Internet - Subsección I De la Custodia de Registros de Conexión Artículo 13.** En la provisión de conexión a Internet, cabe al administrador del sistema autónomo respectivo el deber de mantener los registros de conexión, bajo secreto, en un ambiente controlado y seguro, durante el plazo de un año, según el reglamento. § 1º La responsabilidad de mantener los registros de conexión no puede ser transferida a terceros. § 2º La autoridad policial o administrativa o el Ministerio Público podrá requerir cautelarmente que los registros de conexión sean guardados durante un plazo superior al previsto en este artículo. § 3º En la hipótesis del § 2º, la autoridad solicitante tendrá el plazo de sesenta días, contados a partir de la solicitud, para ingresar, con el pedido de autorización judicial, a los registros previstos en este artículo. § 4º El proveedor responsable de la custodia de los registros deberá mantener el secreto en relación a la solicitud prevista en el § 2º, que perderá su eficacia en caso de que el pedido de autorización judicial no sea aceptado o no haya sido ejecutado en el plazo previsto en el § 3º. § 5º En cualquier caso, la disponibilidad al requirente de los registros de los que trata este artículo deberá ser precedida de una autorización judicial, conforme a lo dispuesto en la Sección IV de este capítulo. § 6º En la aplicación de sanciones por el incumplimiento de lo dispuesto en este artículo, serán considerados la naturaleza, la gravedad de la infracción y los daños resultantes de ella, eventual beneficio para el infractor, las circunstancias agravantes, los antecedentes del infractor y la reincidencia. **Subsección III De la Custodia de Registros de Acceso a Aplicaciones de Internet en la Provisión de Aplicaciones Artículo 15**. El proveedor de aplicaciones de Internet constituido en forma de persona jurídica, que ejerza esa actividad en forma organizada, profesionalmente y con fines económicos, deberá mantener los respectivos registros de acceso a aplicaciones de Internet, en secreto, en ambiente controlado y de seguridad, por el plazo de seis meses, en los términos del reglamento. § 1º Orden judicial podrá obligar, por tiempo determinado, a los proveedores de aplicaciones de Internet, que no estén sujetos a lo dispuesto en el artículo a guardar registros de acceso a aplicaciones de Internet, si se tratan de registros relativos a hechos específicos en un tiempo determinado. § 2º La autoridad policial o administrativa o el Ministerio Público podrán solicitar cautelarmente a cualquier proveedor de aplicaciones de Internet que los registros de acceso a aplicaciones de Internet sean guardados, incluso por plazo superior al previsto en el artículo, observando lo dispuesto en los §§ 3º y 4º del artículo 13. § 3º En cualquier caso, la disponibilidad al requirente, de los registros de los que trata este artículo, deberá ser precedida de autorización judicial, conforme lo dispuesto en la Sección IV de este Capítulo.

Nº	Medidas de investigación	Regulación de medidas de investigación en Brasil
		§ 4º En la aplicación de sanciones por el incumplimiento de lo dispuesto en este artículo, serán considerados la naturaleza y gravedad de la infracción, los daños resultantes de ella, el eventual beneficio para el infractor, las circunstancias agravantes, los antecedentes del infractor y la reincidencia.
3	Mandato de comunicación (Artículo 18 Convenio de Budapest)	**Ley Nº 12.965/2014 - Marco Civil de Internet - Sección II - De la Protección a los Registros, Datos Personales y Comunicaciones Privadas - Artículo 10.** La custodia y entrega de los registros de conexión y de acceso a aplicaciones de Internet de que trata esta ley, así como de los datos personales y del contenido de las comunicaciones privadas, deben atender a la preservación de la intimidad, de la vida privada, de la honra y de la imagen de las partes directa o indirectamente involucradas. § 1º El proveedor responsable de la custodia solamente será obligado a entregar los registros mencionados en el artículo, de forma autónoma o asociados a datos personales u otras informaciones que puedan contribuir a la identificación del usuario o del terminal, mediante orden judicial, tal como queda dispuesto en la Sección IV de este Capítulo, respetando lo dispuesto en el artículo 7º. § 2º El contenido de las comunicaciones privadas solamente podrá ser entregado mediante orden judicial, en los casos y en la forma que establece la ley, respetando lo dispuesto en los párrafos II y III del artículo 7º. § 3º Lo dispuesto en este artículo no impide el acceso, por parte de las autoridades administrativas que detenten competencia legal para su solicitud, a los datos de registro que contengan información personal, filiación y dirección, de acuerdo con la ley. § 4º Las medidas y procedimientos de seguridad y secreto deben ser informados por el responsable de la provisión de servicios de forma clara y atenerse a patrones definidos en reglamento, respetando su derecho de confidencialidad en lo que respecta a secretos empresariales. **Sección IV De la Solicitud Judicial de Registros Artículo 22.** La parte interesada podrá, con el propósito de formar conjunto probatorio en proceso judicial civil o penal, en carácter incidental o autónomo, requerir al juez que ordene al responsable por la guarda u otorgamiento de registros de conexión o de registros de acceso a aplicaciones de Internet. Párrafo único. Sin perjuicio de los demás requisitos legales, el requerimiento deberá contener, bajo pena de inadmisibilidad: I – fundados indicios del acontecimiento del ilícito; II – justificación motivada de la utilidad de los registros solicitados para fines de investigación o instrucción probatoria; y III – período al cual se refieren los registros. **Artículo 23.** Cabe al juez tomar las providencias necesarias a la garantía del sigilo de las informaciones recibidas y a la preservación de la intimidad, de la vida privada, de la honra y de la imagen del usuario, pudiendo determinar secreto de justicia, inclusive en cuanto a los pedidos de custodia de registro.
4	Registro y decomiso de datos informáticos	**No se encontró medida especial aplicable.**

Nº	Medidas de investigación	Regulación de medidas de investigación en Brasil
	almacenados (Artículo 19 Convenio de Budapest)	
5	Recogida en tiempo real de datos de tráfico (Artículo 20 Convenio de Budapest)	**Ley N° 9.296/1996.** Art. 1 La interceptación de comunicaciones telefónicas, de cualquier naturaleza, con fines de prueba en la investigación penal y en la instrucción procesal penal, se ajustará a lo dispuesto en esta Ley y dependerá de la orden del juez competente de la causa principal, bajo secreto judicial. Párrafo unico. Lo dispuesto en esta Ley se aplica a la interceptación del flujo de comunicaciones en sistemas informáticos y telemáticos. [...] *Remitimos el texto completo en honor a la brevedad. Disponible en: https://www.planalto.gov.br/ccivil_03/leis/l9296.htm*
6	Interceptación de datos relativos al contenido (Artículo 21 Convenio de Budapest)	**Ley N° 9.296/1996.** Art. 1 La interceptación de comunicaciones telefónicas, de cualquier naturaleza, con fines de prueba en la investigación penal y en la instrucción procesal penal, se ajustará a lo dispuesto en esta Ley y dependerá de la orden del juez competente de la causa principal, bajo secreto judicial. Párrafo unico. Lo dispuesto en esta Ley se aplica a la interceptación del flujo de comunicaciones en sistemas informáticos y telemáticos. [...] *Remitimos el texto completo en honor a la brevedad. Disponible en: https://www.planalto.gov.br/ccivil_03/leis/l9296.htm*
7	Agente encubierto digital	**No se encontró medida especial aplicable.**
8	Registro remoto	**No se encontró medida especial aplicable.**
9	OSINT	**No se encontró medida especial aplicable.**
10	Acceso transfronterizo de datos	**No se encontró medida especial aplicable.**
11	Hallazgos casuales en evidencia digital	**No se encontró medida especial aplicable.**
12	Desbloqueo compulsivo de datos informáticos	**No se encontró medida especial aplicable.**

Tabla Nº 30: Resumen de medidas de investigación reguladas en Brasil

Como se puede observar en el cuadro, lo más llamativo de la regulación en Brasil es que ninguna de las medidas que hemos encontrado como "aplicables" a las categorías buscadas, las hemos encontrado reguladas en el Código Procesal Penal Federal de Brasil, sino que algunas pertenecen a regulaciones de la Ley de Marco Civil de Internet (que incluye regulación sobre registro de datos) y otras existentes en una vieja normativa del año 1996, destinada a la regulación de la interceptación de comunicaciones.

7.3.4. La conservación de datos

En relación a la conservación de datos, hemos considerado aplicable tanto el artículo 13 como el 15 del Marco Civil de Internet de Brasil. El art. 13 establece la obligación de mantener los registros de conexión, por el plazo de un año, aunque establece que tanto la autoridad policial, administrativa o el Ministerio Público podrán solicitar que el plazo sea superior al previsto para casos concretos.

El inc. 5 de dicho artículo, establece que el acceso a los registros existentes en poder del ISP, deberá ser precedida de una autorización judicial conforme a la sección IV del mismo Capítulo, aspecto que desarrollaremos al analizar el mandato de comunicación de datos.

Por otro lado, en relación a los registros de accesos a aplicaciones de internet en la provisión de aplicaciones, reguladas por el art. 15, se establece que el proveedor de aplicaciones de internet deberá mantener registros de accesos a aplicaciones de internet -en secreto-, por el plazo de seis meses.

Como detalle a comentar, la misma normativa en el artículo 1 establece que en la provisión de conexión, onerosa o gratuita, está prohibido almacenar registros de acceso a aplicaciones de Internet. Es decir, que los proveedores de internet, sólo podrán guardar datos de registros de acceso a internet, pero nunca de aplicaciones.

Asimismo, en el artículo 11 se establece que en cualquier operación de recolección, almacenamiento, protección o tratamiento de registros, datos personales o de comunicaciones por proveedores de conexión y de aplicaciones de

Internet en las que por lo menos uno de estos actos ocurra en territorio nacional, deberá ser obligatoriamente respetada la legislación brasileña, los derechos a la privacidad y a la protección de los datos personales y al secreto de las comunicaciones privadas y de los registros.

No obstante las buenas intenciones del último artículo citado, entendemos que este tipo de regulaciones van en contra de la postura internacional en materia de retención de datos, toda vez que a diferencia de la propuesta antes desarrollada que sugiere el Convenio de Cibercrimen de Budapest (retención o conservación basado en un pedido concreto), aquí la normativa establece la obligación de la guarda de todos los registros por los plazos antes citados (1 año o 6 meses dependen del tipo de dato).

Según ya hemos visto anteriormente en esta tesis, las normativas europeas que establecían obligaciones similares terminaron por considerar inconstitucionales[525] a la luz de una lectura de afectación innecesaria de la privacidad[526] de personas que no tienen ninguna sospecha ni forma parte de ninguna investigación.

7.3.5. La entrega de datos como reemplazado del mandato de comunicacion

A nuestro criterio, la medida sobre el mandato de comunicación la vemos de alguna manera reemplazada a través de la combinación del art. 10 y el art. 22 y 23 del Marco Civil de Internet.

[525] SENTENCIA DEL TRIBUNAL DE JUSTICIA (Gran Sala) de 8 de abril de 2014 (*) «Comunicaciones electrónicas — Directiva 2006/24/CE — Servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones — Conservación de datos generados o tratados en relación con la prestación de tales servicios — Validez — Artículos 7, 8 y 11 de la Carta de los Derechos Fundamentales de la Unión Europea»; Disponible en: https://curia.europa.eu/juris/document/document.jsf?docid=150642&doclang=ES

[526] EURONEWS; “La retención indiscriminada de datos es ilegal, según el TJUE”, Disponible en: https://es.euronews.com/2022/09/20/alemania-privacidad-seguridad

En primer lugar, el art. 10 establece la obligación de custodia y entrega de registros de conexión (y de acceso a aplicaciones) así como los datos personales y contenidos de la comunicación, preservando siempre la intimidad, vida, honra y privacidad de la o las personas involucradas. La entrega de dichos datos será, según el inc. 2, mediante orden judicial siempre de acuerdo a lo previsto en los art. 22 y 23.

Sin embargo, destacamos que el inc. 3 destaca que las autoridades administrativas (policía brasileña por ejemplo) "*podría igualmente acceder a registros que contenga información personal, filiación y dirección, de acuerdo con la ley*". Entendemos que esa inclusión podría ser peligrosa para la privacidad y la intimidad de las personas, ya que generaría la posibilidad del acceso a ciertos registros sin necesidad de contar con la autorización judicial mencionada en el inc. 2.

Continuamos ahora sí haciendo referencia a los arts. 22 y 23, que pertenecen a la Sección IV dedicado precisamente a la "Solicitud Judicial de Registros", donde se define que "*la parte interesada podrá, con el propósito de formar conjunto probatorio en proceso judicial civil o penal, en carácter incidental o autónomo, requerir al juez que ordene al responsable por la guarda u otorgamiento de registros de conexión o de registros de acceso a aplicaciones de Internet*". Ahora bien, celebramos la inclusión acerca de que dicho requerimiento deberá contener obligatoriamente: I – fundados indicios del acontecimiento del ilícito; II – justificación motivada de la utilidad de los registros solicitados para fines de investigación o instrucción probatoria; y III – período al cual se refieren los registros.

Por su parte, el art. 23 incluye la posibilidad de solicitar la garantía del sigilo de las informaciones recibidas y a la preservación de la intimidad, de la vida privada, de la honra y de la imagen del usuario, pudiendo determinar secreto de justicia, inclusive en cuanto a los pedidos de custodia de registro.

7.3.6. La interceptación de las comunicaciones

El art. 1 de la Ley 9.296 establece que la interceptación de comunicaciones telefónicas, de cualquier naturaleza, con fines de prueba en la investigación penal y en la instrucción procesal penal, se ajustará a lo dispuesto en dicha Ley y dependerá de la orden del juez competente de la causa principal, bajo secreto judicial. Asimismo, en el mismo artículo se ha destacado que lo dispuesto en esta Ley se aplica a la interceptación del flujo de comunicaciones en sistemas informáticos y telemáticos, haciendo plena aplicación al destino buscado.

Realizando un breve repaso sobre esta normativa, destacamos que existe una prohibición de realizar interceptación de comunicaciones cuando:

I - no existe evidencia razonable de autoría o participación en un delito penal;

II - la prueba puede ser realizada por otros medios disponibles;

III - el hecho investigado constituye un delito punible, como máximo, con pena de prisión.

En todo caso, deberá describirse claramente la situación objeto de la investigación, incluyendo la indicación y calificaciones de los investigados, salvo que sea claramente imposible, debidamente justificado.

Nuevamente encontramos en Brasil este tipo de normativas que a la primer lectura parecen bastante rigurosas y proteccionistas de los derechos de las personas, pero que, sobre el final, terminan apareciendo algunas excepciones que, a nuestro criterio (-no tenemos certeza sobre la realidad de la práctica en Brasil acerca del nivel de utilización de esta medida-) terminan por desvirtuar la protección, generando casos tan genéricos que permitirían que casi todas las medidas puedan autorizarse (haciendo alguna justificación al respecto).

Avanzando con la normativa, el art. 3 establece que las interceptaciones de las comunicaciones pueden ser ordenadas tanto por la autoridad policial (en investigación criminal) y el representante del Ministerio Público, también en el marco de una investigación criminal e instrucción procesal penal.

Entre los límites encontrados a la medida, destacamos que el art. 5 establece que bajo pena de nulidad, indicando además el método de realización de la investigación, que no podrá exceder de un plazo de quince días, prorrogables por igual período una vez comprobada lo indispensable de la medida.

7.3.7. La captura ambiental de señales electromagnéticas, ópticas o acústicas

A partir de una actualización realizada a partir de la Ley N° 13.964, de 2019, se incorporó la posibilidad que para investigación o instrucción penal, el juez podrá autorizar, a solicitud de la autoridad policial o del Ministerio Público, la captura ambiental de señales electromagnéticas, ópticas o acústicas, cuando: I - la prueba no puede ser realizada por otros medios disponibles e igualmente eficaces; y II - existan pruebas razonables de autoría y participación en delitos cuya pena máxima sea superior a 4 (cuatro) años o en delitos conexos.

De acuerdo al art. 1 la autorización judicial deberá describir detalladamente el lugar y el método de instalación del dispositivo de captura ambiental. La solicitud de esta medida de captura ambiental de señales electromagnéticas, ópticas o acústicas en definitiva entendemos que será la captura de comunicaciones electrónicas (por ejemplo, conexiones de red inalámbricas), o la captura de grabaciones de video que puedan incluir sonido, algo que claramente afectaría la privacidad e intimidad de las personas, máxime instalado de forma ambiental en el exterior, toda vez que de acuerdo al inc. 2 del art. 1, la instalación no podría ser dispuesta dentro de un domicilio. El mismo inciso, establece que para su instalación, podrá instalarse el dispositivo a través de una operación encubierta o nocturna, a fin de evitar llamar la atención con la instalación de la misma.

En relación a los límites de esta medida, el inc. 3 establece que la captura no podrá exceder de los 15 días, renovables por decisión judicial por iguales períodos, siempre comprobando lo indispensable y necesario de dicha medida.

La normativa cierra incorporando como delito penal, la interceptación de comunicaciones informáticos o telemáticas (art. 10), algo que ya hemos desarrollado en el capítulo IV dedicado a la parte material de los delitos informáticos.

7.4. Medidas de investigación reguladas en Colombia

7.4.1. La evolución del marco normativo procesal en Colombia

Colombia ha tenido un gran desarrollo en materia de protección de la privacidad, que como ya hemos visto en la sección del derecho de fondo, la Ley Nº 1.273 del año 2009 "por medio de la cual se modifica el Código Penal un nuevo bien jurídico tutelado – denominado "de la protección de la información y de los datos que contiene una serie de delitos informáticos contemplados en el Convenio de Budapest con especial atención a la protección de datos personales.

Respecto al derecho procesal penal el Código de Procedimiento Penal de Colombia (Ley Nº 9060), tiene desde su reforma en el año 2004 algunas medidas de investigación relacionadas con la obtención de evidencia digital, que con el paso de los años fueron teniendo diversas actualizaciones producto de la generación de jurisprudencia sobre la temática, aspectos que ya veremos a continuación en el desarrollo de algunas de las medidas reguladas.

En el año 2013 el Ministerio de Relaciones Exteriores aceleró las gestiones para ser invitado a adherirse al Convenio de Budapest[527], como parte de la política nacional de ciberseguridad[528]. En Colombia la aprobación de los tratados pasa por la firma del ejecutivo, la aprobación del Congreso y el control de constitucionalidad por

[527] FUNDACIÓN KARISMA. Convenio de Budapest: Aplicación en Colombia frente a Derechos Humanos. 2018. Publicaciones Derechos Digitales. [En línea] <https://www.derechosdigitales.org/publicaciones/convenio-de-budapest-aplicacion-encoombia-frente-a-derechos-humanos/> [Consulta: 01 de julio de 2020]

[528] Planteada mediante documento de Consejo Nacional de Política Social y Económica N°3701 de 2011

parte de la Corte Constitucional. Con fecha 11 de septiembre de 2013 Colombia fue invitada a adherirse al instrumento con un plazo de 5 años para completar la tramitación interna, teniendo hasta el 12 de septiembre de 2020. En junio de 2018 se aprobó la adhesión en Segundo Debate y en 24 de Julio se convirtió en Ley de la República N°1.928. A pesar de esto, no se ha formalizado el ingreso de Colombia ni sus reservas al Convenio de Budapest a la fecha del presente estudio.

A continuación, avanzaremos hacia la identificación de medidas de investigación de nuestro interés dentro del Código Procesal Penal Colombiano:

7.4.2. Cuadro de medidas de investigación reguladas

Nº	Medidas de investigación	Regulación de medidas de investigación en Colombia
1	Conservación inmediata de datos informáticos almacenados (Artículo 16 Convenio de Budapest)	**No se encontró medida especial aplicable.**
2	Conservación y divulgación inmediata de los datos de tráfico (Artículo 17 Convenio de Budapest)	**- Parcialmente aplicable - ARTÍCULO 244. BÚSQUEDA SELECTIVA EN BASES DE DATOS.** La policía judicial, en desarrollo de su actividad investigativa, podrá realizar las comparaciones de datos registradas en bases mecánicas, magnéticas u otras similares, siempre y cuando se trate del simple cotejo de informaciones de acceso público. <Inciso y aparte subrayado CONDICIONALMENTE exequibles> Cuando se requiera adelantar búsqueda selectiva en las bases de datos, que implique el acceso a información confidencial, referida al indiciado o imputado o, inclusive a la obtención de datos derivados del análisis cruzado de las mismas, deberá mediar autorización previa del fiscal que dirija la investigación y se aplicarán, en lo pertinente, las disposiciones relativas a los registros y allanamientos. En estos casos, la revisión de la legalidad se realizará ante el juez de control de garantías, dentro de las treinta y seis (36) horas siguientes a la culminación de la búsqueda selectiva de la información. PARÁGRAFO 1o. <Parágrafo adicionado por el artículo 18 de la Ley 1908 de 2018. El nuevo texto es el siguiente:> Los términos para la búsqueda selectiva en base de datos en las investigaciones que se adelanten contra miembros de

Nº	Medidas de investigación	Regulación de medidas de investigación en Colombia
		Grupos Delictivos Organizados y Grupos Armados Organizados en etapa de indagación serán de seis (6) meses y en investigación de tres (3) meses, prorrogables hasta por un término igual. PARÁGRAFO 2o. <Parágrafo adicionado por el artículo 18 de la Ley 1908 de 2018. El nuevo texto es el siguiente:> En las investigaciones que se sigan contra Organizaciones Criminales, el Juez de Control de Garantías podrá autorizar el levantamiento de la reserva y el acceso a la totalidad de bases de datos en las cuales pueda encontrarse el indiciado o imputado, cuando así se justifique por las circunstancias del caso y el tipo de conducta punible que se investiga. Esta autorización se concederá por un término igual al contemplado en el parágrafo primero, al término del cual, dentro de las treinta y seis horas siguientes al último acto de investigación se debe acudir nuevamente ante el juez de control de garantías, con el fin de solicitar sea impartida legalidad a la totalidad del procedimiento.
3	Mandato de comunicación (Artículo 18 Convenio de Budapest)	**ARTÍCULO 236. RECUPERACIÓN DE INFORMACIÓN PRODUCTO DE LA TRANSMISIÓN DE DATOS A TRAVÉS DE LAS REDES DE COMUNICACIONES.** <Artículo modificado por el artículo 53 de la Ley 1453 de 2011. El nuevo texto es el siguiente:> Cuando el fiscal tenga motivos razonablemente fundados, de acuerdo con los medios cognoscitivos previstos en este código, para inferir que el indiciado o imputado está transmitiendo o manipulando datos a través de las redes de telecomunicaciones, ordenará a policía judicial la retención, aprehensión o recuperación de dicha información, equipos terminales, dispositivos o servidores que pueda haber utilizado cualquier medio de almacenamiento físico o virtual, análogo o digital, para que expertos en informática forense, descubran, recojan, analicen y custodien la información que recuperen; lo anterior con el fin de obtener elementos materiales probatorios y evidencia física o realizar la captura del indiciado, imputado o condenado. En estos casos serán aplicables analógicamente, según la naturaleza de este acto, los criterios establecidos para los registros y allanamientos. La aprehensión de que trata este artículo se limitará exclusivamente al tiempo necesario para la captura de la información en él contenida. Inmediatamente se devolverán los equipos incautados, de ser el caso. PARÁGRAFO. <Parágrafo adicionado por el artículo 14 de la Ley 1908 de 2018. El nuevo texto es el siguiente:> Cuando se trate de investigaciones contra miembros de Grupos Delictivos Organizados y Grupos Armados Organizados, la Policía Judicial dispondrá de un término de seis (6) meses en etapa de indagación y tres (3) meses en etapa de investigación, para que expertos en informática forense identifiquen, sustraigan, recojan, analicen y custodien la información que recuperen."
4	Registro y decomiso de datos informáticos	**ARTÍCULO 236. RECUPERACIÓN DE INFORMACIÓN PRODUCTO DE LA TRANSMISIÓN DE DATOS A TRAVÉS DE LAS REDES DE COMUNICACIONES.** <Artículo modificado por el artículo 53 de la Ley 1453 de

Nº	Medidas de investigación	Regulación de medidas de investigación en Colombia
	almacenados (Artículo 19 Convenio de Budapest)	2011. El nuevo texto es el siguiente:> Cuando el fiscal tenga motivos razonablemente fundados, de acuerdo con los medios cognoscitivos previstos en este código, para inferir que el indiciado o imputado está transmitiendo o manipulando datos a través de las redes de telecomunicaciones, ordenará a policía judicial la retención, aprehensión o recuperación de dicha información, equipos terminales, dispositivos o servidores que pueda haber utilizado cualquier medio de almacenamiento físico o virtual, análogo o digital, para que expertos en informática forense, descubran, recojan, analicen y custodien la información que recuperen; lo anterior con el fin de obtener elementos materiales probatorios y evidencia física o realizar la captura del indiciado, imputado o condenado. En estos casos serán aplicables analógicamente, según la naturaleza de este acto, los criterios establecidos para los registros y allanamientos. La aprehensión de que trata este artículo se limitará exclusivamente al tiempo necesario para la captura de la información en él contenida. Inmediatamente se devolverán los equipos incautados, de ser el caso. PARÁGRAFO. <Parágrafo adicionado por el artículo 14 de la Ley 1908 de 2018. El nuevo texto es el siguiente:> Cuando se trate de investigaciones contra miembros de Grupos Delictivos Organizados y Grupos Armados Organizados, la Policía Judicial dispondrá de un término de seis (6) meses en etapa de indagación y tres (3) meses en etapa de investigación, para que expertos en informática forense identifiquen, sustraigan, recojan, analicen y custodien la información que recuperen. **ARTÍCULO 244. BÚSQUEDA SELECTIVA EN BASES DE DATOS.** La policía judicial, en desarrollo de su actividad investigativa, podrá realizar las comparaciones de datos registradas en bases mecánicas, magnéticas u otras similares, siempre y cuando se trate del simple cotejo de informaciones de acceso público. <Inciso y aparte subrayado CONDICIONALMENTE exequibles> Cuando se requiera adelantar búsqueda selectiva en las bases de datos, que implique el acceso a información confidencial, referida al indiciado o imputado o, inclusive a la obtención de datos derivados del análisis cruzado de las mismas, deberá mediar autorización previa del fiscal que dirija la investigación y se aplicarán, en lo pertinente, las disposiciones relativas a los registros y allanamientos. En estos casos, la revisión de la legalidad se realizará ante el juez de control de garantías, dentro de las treinta y seis (36) horas siguientes a la culminación de la búsqueda selectiva de la información. PARÁGRAFO 1o. <Parágrafo adicionado por el artículo 18 de la Ley 1908 de 2018. El nuevo texto es el siguiente:> Los términos para la búsqueda selectiva en base de datos en las investigaciones que se adelanten contra miembros de Grupos Delictivos Organizados y Grupos Armados Organizados en etapa de indagación serán de seis (6) meses y en investigación de tres (3) meses,

Nº	Medidas de investigación	Regulación de medidas de investigación en Colombia
		prorrogables hasta por un término igual. PARÁGRAFO 2o. <Parágrafo adicionado por el artículo 18 de la Ley 1908 de 2018. El nuevo texto es el siguiente:> En las investigaciones que se sigan contra Organizaciones Criminales, el Juez de Control de Garantías podrá autorizar el levantamiento de la reserva y el acceso a la totalidad de bases de datos en las cuales pueda encontrarse el indiciado o imputado, cuando así se justifique por las circunstancias del caso y el tipo de conducta punible que se investiga. Esta autorización se concederá por un término igual al contemplado en el parágrafo primero, al término del cual, dentro de las treinta y seis horas siguientes al último acto de investigación se debe acudir nuevamente ante el juez de control de garantías, con el fin de solicitar sea impartida legalidad a la totalidad del procedimiento.
5	Recogida en tiempo real de datos de tráfico (Artículo 20 Convenio de Budapest)	**ARTÍCULO 235. INTERCEPTACIÓN DE COMUNICACIONES.** <Artículo modificado por el artículo 52 de la Ley 1453 de 2011. El nuevo texto es el siguiente:> El fiscal podrá ordenar, con el objeto de buscar elementos materiales probatorios, evidencia física, búsqueda y ubicación de imputados, indiciados o condenados, que se intercepten mediante grabación magnetofónica o similares las comunicaciones que se cursen por cualquier red de comunicaciones, en donde curse información o haya interés para los fines de la actuación. En este sentido, las autoridades competentes serán las encargadas de la operación técnica de la respectiva interceptación así como del procesamiento de la misma. Tienen la obligación de realizarla inmediatamente después de la notificación de la orden y todos los costos serán a cargo de la autoridad que ejecute la interceptación. En todo caso, deberá fundamentarse por escrito. Las personas que participen en estas diligencias se obligan a guardar la debida reserva. Por ningún motivo se podrán interceptar las comunicaciones del defensor. La orden tendrá una vigencia máxima de seis (6) meses, pero podrá prorrogarse, a juicio del fiscal, subsisten los motivos fundados que la originaron. La orden del fiscal de prorrogar la interceptación de comunicaciones y similares deberá someterse al control previo de legalidad por parte del Juez de Control de Garantías. PARÁGRAFO. <Parágrafo adicionado por el artículo 13 de la Ley 1908 de 2018. El nuevo texto es el siguiente:> Los funcionarios de Policía Judicial deberán rendir informes parciales de los resultados de la interceptación de comunicaciones cuando dentro de las mismas se establezcan informaciones que ameriten una actuación inmediata para recolectar evidencia o elementos materiales probatorios e impedir la comisión de otra u otras conductas delictivas. En todo caso, el fiscal comparecerá ante el juez de control de garantías a efectos de legalizar las actuaciones cuando finalice la actividad investigativa.
6	Interceptación de	**ARTÍCULO 235. INTERCEPTACIÓN DE COMUNICACIONES.** <Artículo

Nº	Medidas de investigación	Regulación de medidas de investigación en Colombia
	datos relativos al contenido (Artículo 21 Convenio de Budapest)	modificado por el artículo 52 de la Ley 1453 de 2011. El nuevo texto es el siguiente:> El fiscal podrá ordenar, con el objeto de buscar elementos materiales probatorios, evidencia física, búsqueda y ubicación de imputados, indiciados o condenados, que se intercepten mediante grabación magnetofónica o similares las comunicaciones que se cursen por cualquier red de comunicaciones, en donde curse información o haya interés para los fines de la actuación. En este sentido, las autoridades competentes serán las encargadas de la operación técnica de la respectiva interceptación así como del procesamiento de la misma. Tienen la obligación de realizarla inmediatamente después de la notificación de la orden y todos los costos serán a cargo de la autoridad que ejecute la interceptación. En todo caso, deberá fundamentarse por escrito. Las personas que participen en estas diligencias se obligan a guardar la debida reserva. Por ningún motivo se podrán interceptar las comunicaciones del defensor. La orden tendrá una vigencia máxima de seis (6) meses, pero podrá prorrogarse, a juicio del fiscal, subsisten los motivos fundados que la originaron. La orden del fiscal de prorrogar la interceptación de comunicaciones y similares deberá someterse al control previo de legalidad por parte del Juez de Control de Garantías. PARÁGRAFO. <Parágrafo adicionado por el artículo 13 de la Ley 1908 de 2018. El nuevo texto es el siguiente:> Los funcionarios de Policía Judicial deberán rendir informes parciales de los resultados de la interceptación de comunicaciones cuando dentro de las mismas se establezcan informaciones que ameriten una actuación inmediata para recolectar evidencia o elementos materiales probatorios e impedir la comisión de otra u otras conductas delictivas. En todo caso, el fiscal comparecerá ante el juez de control de garantías a efectos de legalizar las actuaciones cuando finalice la actividad investigativa.
7	Agente encubierto digital	**ARTÍCULO 242B. OPERACIONES ENCUBIERTAS EN MEDIOS DE COMUNICACIÓN VIRTUAL.** <Artículo adicionado por el artículo 16 de la Ley 1908 de 2018. El nuevo texto es el siguiente:> La técnica especial de investigación de agente encubierto contemplada en el artículo 242 podrá utilizarse cuando se verifique la posible existencia de hechos constitutivos de delitos cometidos por organizaciones criminales que actúan a través de comunicaciones mantenidas en canales cerrados de comunicación virtual. El agente encubierto podrá intercambiar o enviar archivos ilícitos por razón de su contenido y analizar los resultados de los algoritmos aplicados para la identificación de dichos archivos ilícitos. También obtener imágenes y grabaciones de las conversaciones que puedan mantenerse en los encuentros previstos entre la gente y el indiciado. PARÁGRAFO. En todo caso, tratándose de este tipo de operaciones encubiertas, se deberá contar con una autorización previa por parte del Juez de

Nº	Medidas de investigación	Regulación de medidas de investigación en Colombia
		Control de Garantías para interferir en las comunicaciones, de conformidad con lo dispuesto en la jurisprudencia constitucional.
8	Registro remoto	**No se encontró medida especial aplicable.**
9	OSINT	**No se encontró medida especial aplicable.**
10	Acceso transfronterizo de datos	**No se encontró medida especial aplicable.**
11	Hallazgos casuales en evidencia digital	**No se encontró medida especial aplicable.**
12	Desbloqueo compulsivo de datos informáticos	**No se encontró medida especial aplicable.**

Tabla Nº 31: Resumen de medidas de investigación reguladas en Colombia

7.4.3. Búsqueda selectiva en bases de datos

Como habíamos adelantado en la introducción, si bien el Código Procesal Penal Colombiano tuvo su reestructuración más fuerte en el año 2004 (Ley Nº 9060), a lo largo de los años, se han realizado distintas actualizaciones y mejoras, de acuerdo a la evolución de la jurisprudencia en algunos casos y por necesidad tecnológica en otros.

A modo ejemplo, la formulación original del art. 244 sobre búsqueda selectiva en bases de datos, tuvo dos sentencias de la Corte Constitucional. Una primera sentencia[529] donde el Magistrado Ponente Dr. Jaime Córdoba Triviño, "*en el entendido que se requiere de orden judicial previa cuando se trata de datos personales organizados con fines legales y recogidos por instituciones o entidades públicas o privadas debidamente autorizadas para ello*".

[529] CORTE CONSTITUCIONAL DE COLOMBIA, Sentencia C-336-07 de 9 de mayo de 2007,

Una segunda sentencia[530] donde el Magistrado Ponente Dr. Rodrigo Escobar Gil expresó "*...siempre que se entienda que cuando el indiciado tenga noticia de que en las diligencias practicadas en la etapa de indagación anterior a la formulación de la imputación, se está investigando su participación en la comisión de un hecho punible, el juez de control de garantías debe autorizarle su participación y la de su abogado en la audiencia posterior de control de legalidad de tales diligencias, si así lo solicita*".

Lo primero que puede llamarnos la atención es que en la regulación actual del art. 244 se establece que cuando se requiera adelantar búsqueda selectiva en las bases de datos, que implique el acceso a información confidencial referida al imputado, podrá realizarse con autorización previa del fiscal que dirija la investigación. Es decir, que en principio no se menciona la necesidad de autorización judicial. No obstante, párrafo posterior establece que "*En estos casos, la revisión de la legalidad se realizará ante el juez de control de garantías, dentro de las treinta y seis (36) horas siguientes a la culminación de la búsqueda selectiva de la información.*"

En el 2018 se agregó un nuevo párrafo que determinar que "*Los términos para la búsqueda selectiva en base de datos en las investigaciones que se adelanten contra miembros de Grupos Delictivos Organizados y Grupos Armados Organizados en etapa de indagación serán de seis (6) meses y en investigación de tres (3) meses, prorrogables hasta por un término igual*".

Existió algunas discusiones en Colombia acerca de si era posible que la defensa penal se encuentre legitimada para realizar Búsquedas Selectivas en Bases de Datos en el proceso penal[531]. Si bien esta es una actividad que en principio estaba concebida únicamente para la Fiscalía, cada vez más es una herramienta útil para que la defensa pueda acceder a información que le permita demostrar su teoría del caso.

[530] CORTE CONSTITUCIONAL DE COLOMBIA, Sentencia C-025-09 de 27 de enero de 2009
[531] PANTOJA RUIZ, Juan Pablo; "BSBD por la defensa en el proceso penal"; Disponible en: https://www.asuntoslegales.com.co/consultorio/bsbd-por-la-defensa-en-el-proceso-penal-3418941

Actualmente hay consenso (también por la aplicación del principio de igualdad de armas) sobre que esta actividad presenta una serie de cargas (que los jueces parecen aplicar con mayor severidad a los defensores). Las sentencias C-186 de 2008, C-536 de 2008 y el Auto con radicado 35.432 de 2010 (MP Sigifredo Espinosa Pérez) han autorizado a la defensa para adelantar actos de investigación en igualdad de armas a la Fiscalía, incluida la medida de Búsquedas Selectivas en Bases de Datos.

A través de la sentencia C-336 de 2007[532] hace obligatorio acudir a un juez de control de garantías para obtener control previo a la medida de Búsquedas Selectivas en Bases de Dato, la haga la Fiscalía o la defensa, bajo el desarrollo que toda búsqueda de datos afecta la intimidad. Esta sentencia produjo una guía de audiencia que se recomienda observar para tener respuestas favorables a esta medida: (i) exponer clara y detalladamente los motivos fundados y su respaldo de medios cognoscitivos (Art.220-221 del CPP), (ii) precisar qué información se pretende obtener, (iii) exponer que se trata de información confidencial contenida en bases de datos que no son de acceso público (Leyes 1266, 1581 y/o 1712) y (iv) realizar un juicio de proporcionalidad (idoneidad, necesidad y proporcionalidad estricta).

Para el autor Pantoja Ruiz, la defensa al momento de realizar su pedido debe sustentar aportando, cuanto menos: (i) elementos materiales de prueba que sustenten su recuento fáctico y/o su teoría del caso y (ii) la orden a investigador que solicita sea avalada por el juez de control de garantías.

Cuando el artículo 244 remite a las normas de registro y allanamiento, es necesario remitirse a los artículos 220 y 221 del CPP. Estos artículos imponen el deber de acreditar un "motivo razonablemente fundado" para que se avale la Búsquedas Selectivas en Bases de Datos, lo que traduce que la teoría del caso (tanto de la fiscalía como de la defensa) debería estar suficientemente sustentada en elementos materiales de prueba. Esta es la carga más compleja que ha de acreditar

[532] Sentencia C-336 de 2007 Corte Constitucional; Disponible en: https://www.corteconstitucional.gov.co/relatoria/2007/C-336-07.htm#:~:text=La%20b%C3%BAsqueda%20selectiva%20de%20informaci%C3%B3n,Estado%20debe%20preservar%20para%20la

el solicitante, pues ha de demostrar que la información a la que pretende acceder guarda coherencia con los hechos y su teoría del caso.

7.4.4. La posibilidad de recuperación de información

Colombia regula en su artículo 236 del Código Procesal Penal una medida definida como "recuperación de información producto de la transmisión de datos a través de las redes de comunicación" que antiguamente se limitaba a la aprehensión física del hardware utilizado en el supuesto delito, pero que en la actualidad, permite el secuestro tanto de la información, como de los equipos o dispositivos utilizados para el almacenamiento de la información.

En el 2011, el artículo fue modificado agregándose que cuando el fiscal tenga motivos razonablemente fundados, que la persona investigada está transmitiendo o manipulando datos a través de las redes de telecomunicaciones, podrá ordenar a policía judicial la retención, aprehensión o recuperación de dicha información, equipos terminales, dispositivos o servidores que pueda haber utilizado cualquier medio de almacenamiento físico o virtual, análogo o digital, para que expertos en informática forense, descubran, recojan, analicen y custodien la información que recuperen; lo anterior con el fin de obtener elementos materiales probatorios y evidencia física o realizar la captura del indiciado, imputado o condenado.

El tercer párrafo incluye como límite acerca de que la aprehensión de los equipos se limitará exclusivamente al tiempo necesario para la captura de la información existente en dichos equipos, es decir, el tiempo necesario para realizar las respectivas extracciones forenses. Realizadas las mismas, el código establece la devolución de los equipos incautados.

Por último, en el 2018, se agregó el caso que cuando se trate de investigaciones contra miembros de Grupos Delictivos Organizados y Grupos Armados Organizados, la Policía Judicial dispondrá de un término de seis (6) meses en etapa de indagación y tres (3) meses en etapa de investigación, para que expertos en informática forense identifiquen, sustraigan, recojan, analicen y

custodien la información que recuperen. Es decir, para estos casos en particular, el propio Código dispone de un tiempo límite para realizar la extracción de información, algo que, dependiendo del caso (y la saturación de los propios laboratorios forenses) podría incluso jugar en contra de la propia fiscalía.

7.4.5. La interceptación de comunicaciones

Al momento de su adhesión al Convenio de Budapest, Colombia efectuó reservas sobre el artículo 20 y otra sobre el artículo 21 relacionado justamente al tema de la recolección de datos en tiempo real e intervención de comunicaciones. Estas reservas consisten en limitar la aplicación de la medida de obtención en tiempo real de datos relativos al tráfico para que procese sólo respecto de delitos determinados. Sin embargo, no se señaló a qué delitos se limita la aplicación de tal medida, por lo que quedó una reserva sin aplicación concreta.

La otra reserva, sobre la interceptación de datos relativos al tráfico, se refiere a que la medida es procedente sólo en casos de que un sistema informático se haya puesto en funcionamiento para un grupo restringido de usuarios además de que no emplee las redes públicas de telecomunicación y no esté conectado a otro sistema informático, ya sea público o privado.

El artículo 235, modificado por la Ley 1453 de 2011, habilita al fiscal a ordenar que se intercepten mediante grabación magnetofónica o similares las comunicaciones que se cursen por cualquier red de comunicaciones, en donde curse información o haya interés para los fines de la actuación. El artículo incluye en su inc. 3 que por ningún motivo se podrán interceptar las comunicaciones del defensor.

A nivel de límites, la orden tendrá una vigencia máxima de seis (6) meses, pero podrá prorrogarse, a juicio del fiscal, subsisten los motivos fundados que la originaron. La orden del fiscal de prorrogar la interceptación de comunicaciones y similares deberá someterse al control previo de legalidad por parte del Juez de Control de Garantías.

En el año 2018, se agregó un nuevo párrafo final que indica que los funcionarios de Policía Judicial deberán rendir informes parciales de los resultados de la interceptación de comunicaciones cuando dentro de las mismas se establezcan informaciones que ameriten una actuación inmediata para recolectar evidencia o elementos materiales probatorios e impedir la comisión de otra u otras conductas delictivas.

7.4.6. Operaciones encubiertas en medios de comunicación virtual

A través de una actualización realizada en el año 2018, a través de la Ley Nº 1908, Colombia habilitó formalmente que la técnica especial de investigación de agente encubierto contemplada en el artículo 242[533] podrá utilizarse cuando se verifique la posible existencia de hechos constitutivos de delitos cometidos por organizaciones criminales que actúan a través de comunicaciones mantenidas en canales cerrados de comunicación virtual.

Para estos casos, la figura habilita que el agente encubierto pueda intercambiar o enviar archivos ilícitos por razón de su contenido, una herramienta útil como hemos dicho antes, para algunos tipos de investigaciones donde para formar parte de un grupo, es necesario intercambiar contenidos, como suele sucede con las redes de distribución o comercialización de material de abuso sexual infantil.

[533] *ARTÍCULO 242. ACTUACIÓN DE AGENTES ENCUBIERTOS. Cuando el fiscal tuviere motivos razonablemente fundados, de acuerdo con los medios cognoscitivos previstos en este código, para inferir que el indiciado o el imputado en la investigación que se adelanta, continúa desarrollando una actividad criminal, previa autorización del Director Nacional o Seccional de Fiscalías, podrá ordenar la utilización de agentes encubiertos, siempre que resulte indispensable para el éxito de las tareas investigativas. En desarrollo de esta facultad especial podrá disponerse que uno o varios funcionarios de la policía judicial o, incluso particulares, puedan actuar en esta condición y realizar actos extrapenales con trascendencia jurídica. En consecuencia, dichos agentes estarán facultados para intervenir en el tráfico comercial, asumir obligaciones, ingresar y participar en reuniones en el lugar de trabajo o domicilio del indiciado o imputado y, si fuere necesario, adelantar transacciones con él. Igualmente, si el agente encubierto encuentra que en los lugares donde ha actuado existe información útil para los fines de la investigación, lo hará saber al fiscal para que este disponga el desarrollo de una operación especial, por parte de la policía judicial, con miras a que se recoja la información y los elementos materiales probatorios y evidencia física hallados. [...]*

En el párrafo final, se agregó a forma de requisito, que tratándose de este tipo de operaciones encubiertas, se deberá contar con una autorización previa por parte del Juez de Control de Garantías.

7.5. Medidas de investigación reguladas en México

7.5.1. El Código Nacional de Procedimientos Penales Mexicano

Con la reforma constitucional en materia de seguridad y justicia publicada en el Diario Oficial de la Federación el 18 de junio de 2008, el Constituyente Permanente estableció el tránsito desde el sistema mixto de justicia penal hacia un sistema de corte acusatorio-oral.

En ese contexto, el 8 de octubre de 2013 se publicó en el Diario Oficial de la Federación la reforma al artículo 73, fracción XXI de la Constitución Política de los Estados Unidos Mexicanos que facultó al Congreso de la Unión a expedir la legislación única en materia procedimental penal, de mecanismos alternativos de solución de controversias y de ejecución de penas que regirán en la República en el orden común y federal.

El Código Nacional de Procedimientos Penales fue publicado en el Diario Oficial de la Federación el 5 de marzo de 2014 y es de observancia general en toda la República Mexicana tratándose de delitos que sean competencia de los órganos jurisdiccionales federales y locales.

En este ordenamiento se establecen las normas aplicables a la investigación de un hecho que la ley señale como delito, a la competencia e incompetencia de los órganos jurisdiccionales y a las formalidades de los actos procedimentales (audiencias, notificaciones, citaciones y plazos).

El código también contiene disposiciones aplicables a los sujetos del proceso penal (víctima u ofendido, imputado, defensor, Ministerio Público, policía, jueces y

magistrados), a las pruebas, a la deliberación, al fallo y a la sentencia. Este cuerpo normativo contempla los recursos de revocación y apelación. Y contiene disposiciones tratándose de procedimientos para personas inimputables y procedimientos especiales para pueblos y comunidades indígenas, y personas jurídicas.

7.5.2. Cuadro de medidas de investigación reguladas

Nº	Medidas de investigación	Regulación de medidas de investigación en México
1	Conservación inmediata de datos informáticos almacenados (Artículo 16 Convenio de Budapest)	**Artículo 303. Localización geográfica en tiempo real y solicitud de entrega de datos conservados:** Cuando el Ministerio Público considere necesaria la localización geográfica en tiempo real o entrega de datos conservados por los concesionarios de telecomunicaciones, los autorizados o proveedores de servicios de aplicaciones y contenidos de los equipos de comunicación móvil asociados a una línea que se encuentra relacionada con los hechos que se investigan, el Procurador, o el servidor público en quien se delegue la facultad, podrá solicitar al Juez de control del fuero correspondiente en su caso, por cualquier medio, requiera a los concesionarios de telecomunicaciones, los autorizados o proveedores de servicios de aplicaciones y contenidos, para que proporcionen con la oportunidad y suficiencia necesaria a la autoridad investigadora, la información solicitada para el inmediato desahogo de dichos actos de investigación. Los datos conservados a que refiere este párrafo se destruirán en caso de que no constituyan medio de prueba idóneo o pertinente. En la solicitud se expresarán los equipos de comunicación móvil relacionados con los hechos que se investigan, señalando los motivos e indicios que sustentan la necesidad de la localización geográfica en tiempo real o la entrega de los datos conservados, su duración y, en su caso, la denominación de la empresa autorizada o proveedora del servicio de telecomunicaciones a través del cual se operan las líneas, números o aparatos que serán objeto de la medida. La petición deberá ser resuelta por la autoridad judicial de manera inmediata por cualquier medio que garantice su autenticidad, o en audiencia privada con la sola comparecencia del Ministerio Público. Si la resolución se emite o registra por medios diversos al escrito, los puntos resolutivos de la orden deberán transcribirse y entregarse al Ministerio Público. En caso de que el Juez de control niegue la orden de localización geográfica en tiempo real o la entrega de los datos conservados, el Ministerio Público podrá subsanar las deficiencias y solicitar nuevamente la orden o podrá apelar la decisión. En este caso la apelación debe ser resuelta en un plazo no mayor de doce horas a partir de que se interponga. Excepcionalmente, cuando esté en peligro la integridad física o la vida de una persona o se encuentre en riesgo el objeto del delito, así como en hechos relacionados con la privación ilegal de la libertad, secuestro, extorsión o

Nº	Medidas de investigación	Regulación de medidas de investigación en México
		delincuencia organizada, el Procurador, o el servidor público en quien se delegue la facultad, bajo su más estricta responsabilidad, ordenará directamente la localización geográfica en tiempo real o la entrega de los datos conservados a los concesionarios de telecomunicaciones, los autorizados o proveedores de servicios de aplicaciones y contenidos, quienes deberán atenderla de inmediato y con la suficiencia necesaria. A partir de que se haya cumplimentado el requerimiento, el Ministerio Público deberá informar al Juez de control competente por cualquier medio que garantice su autenticidad, dentro del plazo de cuarenta y ocho horas, a efecto de que ratifique parcial o totalmente de manera inmediata la subsistencia de la medida, sin perjuicio de que el Ministerio Público continúe con su actuación. Cuando el Juez de control no ratifique la medida a que hace referencia el párrafo anterior, la información obtenida no podrá ser incorporada al procedimiento penal. Asimismo el Procurador, o el servidor público en quien se delegue la facultad podrá requerir a los sujetos obligados que establece la Ley Federal de Telecomunicaciones y Radiodifusión, la conservación inmediata de datos contenidos en redes, sistemas o equipos de informática, hasta por un tiempo máximo de noventa días, lo cual deberá realizarse de forma inmediata. La solicitud y entrega de los datos contenidos en redes, sistemas o equipos de informática se llevará a cabo de conformidad por lo previsto por este artículo. Lo anterior sin menoscabo de las obligaciones previstas en materia de conservación de información para las concesionarias y autorizados de telecomunicaciones en términos del artículo 190, fracción II de la Ley Federal de Telecomunicaciones y Radiodifusión. Artículo reformado DOF 17-06-2016
2	Conservación y divulgación inmediata de los datos de tráfico (Artículo 17 Convenio de Budapest)	**Artículo 303. Localización geográfica en tiempo real y solicitud de entrega de datos conservados:** Cuando el Ministerio Público considere necesaria la localización geográfica en tiempo real o entrega de datos conservados por los concesionarios de telecomunicaciones, los autorizados o proveedores de servicios de aplicaciones y contenidos de los equipos de comunicación móvil asociados a una línea que se encuentra relacionada con los hechos que se investigan, el Procurador, o el servidor público en quien se delegue la facultad, podrá solicitar al Juez de control del fuero correspondiente en su caso, por cualquier medio, requiera a los concesionarios de telecomunicaciones, los autorizados o proveedores de servicios de aplicaciones y contenidos, para que proporcionen con la oportunidad y suficiencia necesaria a la autoridad investigadora, la información solicitada para el inmediato desahogo de dichos actos de investigación. Los datos conservados a que refiere este párrafo se destruirán en caso de que no constituyan medio de prueba idóneo o pertinente. En la solicitud se expresarán los equipos de comunicación móvil relacionados con los hechos que se investigan, señalando los motivos e indicios que sustentan la necesidad de la localización geográfica en tiempo real o la entrega de los datos conservados, su duración y, en su caso, la denominación de la empresa autorizada o proveedora del servicio de telecomunicaciones a través del cual se operan las líneas, números o aparatos que serán objeto de la medida.

Nº	Medidas de investigación	Regulación de medidas de investigación en México
		La petición deberá ser resuelta por la autoridad judicial de manera inmediata por cualquier medio que garantice su autenticidad, o en audiencia privada con la sola comparecencia del Ministerio Público. Si la resolución se emite o registra por medios diversos al escrito, los puntos resolutivos de la orden deberán transcribirse y entregarse al Ministerio Público. En caso de que el Juez de control niegue la orden de localización geográfica en tiempo real o la entrega de los datos conservados, el Ministerio Público podrá subsanar las deficiencias y solicitar nuevamente la orden o podrá apelar la decisión. En este caso la apelación debe ser resuelta en un plazo no mayor de doce horas a partir de que se interponga. Excepcionalmente, cuando esté en peligro la integridad física o la vida de una persona o se encuentre en riesgo el objeto del delito, así como en hechos relacionados con la privación ilegal de la libertad, secuestro, extorsión o delincuencia organizada, el Procurador, o el servidor público en quien se delegue la facultad, bajo su más estricta responsabilidad, ordenará directamente la localización geográfica en tiempo real o la entrega de los datos conservados a los concesionarios de telecomunicaciones, los autorizados o proveedores de servicios de aplicaciones y contenidos, quienes deberán atenderla de inmediato y con la suficiencia necesaria. A partir de que se haya cumplimentado el requerimiento, el Ministerio Público deberá informar al Juez de control competente por cualquier medio que garantice su autenticidad, dentro del plazo de cuarenta y ocho horas, a efecto de que ratifique parcial o totalmente de manera inmediata la subsistencia de la medida, sin perjuicio de que el Ministerio Público continúe con su actuación. Cuando el Juez de control no ratifique la medida a que hace referencia el párrafo anterior, la información obtenida no podrá ser incorporada al procedimiento penal. Asimismo el Procurador, o el servidor público en quien se delegue la facultad podrá requerir a los sujetos obligados que establece la Ley Federal de Telecomunicaciones y Radiodifusión, la conservación inmediata de datos contenidos en redes, sistemas o equipos de informática, hasta por un tiempo máximo de noventa días, lo cual deberá realizarse de forma inmediata. La solicitud y entrega de los datos contenidos en redes, sistemas o equipos de informática se llevará a cabo de conformidad por lo previsto por este artículo. Lo anterior sin menoscabo de las obligaciones previstas en materia de conservación de información para las concesionarias y autorizados de telecomunicaciones en términos del artículo 190, fracción II de la Ley Federal de Telecomunicaciones y Radiodifusión. Artículo reformado DOF 17-06-2016
3	Mandato de comunicación (Artículo 18 Convenio de Budapest)	**- Parcialmente aplicable - Artículo 301. Colaboración con la autoridad:** Los concesionarios, permisionarios y demás titulares de los medios o sistemas susceptibles de intervención, deberán colaborar eficientemente con la autoridad competente para el desahogo de dichos actos de investigación, de conformidad con las disposiciones aplicables. Asimismo, deberán contar con la capacidad técnica indispensable que atienda las exigencias requeridas por la autoridad judicial para operar una orden de intervención de comunicaciones privadas.

Nº	Medidas de investigación	Regulación de medidas de investigación en México
		El incumplimiento a este mandato será sancionado conforme a las disposiciones penales aplicables **Artículo 276. Aportación de comunicaciones entre particulares** Las comunicaciones entre particulares podrán ser aportadas voluntariamente a la investigación o al proceso penal, cuando hayan sido obtenidas directamente por alguno de los participantes en la misma. Las comunicaciones aportadas por los particulares deberán estar estrechamente vinculadas con el delito que se investiga, por lo que en ningún caso el juez admitirá comunicaciones que violen el deber de confidencialidad respecto de los sujetos a que se refiere este Código, ni la autoridad prestará el apoyo a que se refiere el párrafo anterior cuando se viole dicho deber. No se viola el deber de confidencialidad cuando se cuente con el consentimiento expreso de la persona con quien se guarda dicho deber.
4	Registro y decomiso de datos informáticos almacenados (Artículo 19 Convenio de Budapest)	**- Parcialmente aplicable -** **Artículo 291. Intervención de las comunicaciones privadas:** Cuando en la investigación el Ministerio Público considere necesaria la intervención de comunicaciones privadas, el Titular de la Procuraduría General de la República, o en quienes éste delegue esta facultad, así como los Procuradores de las entidades federativas, podrán solicitar al Juez federal de control competente, por cualquier medio, la autorización para practicar la intervención, expresando el objeto y necesidad de la misma. Párrafo reformado DOF 17-06-2016 La intervención de comunicaciones privadas, abarca todo sistema de comunicación, o programas que sean resultado de la evolución tecnológica, que permitan el intercambio de datos, informaciones, audio, video, mensajes, así como archivos electrónicos que graben, conserven el contenido de las conversaciones o registren datos que identifiquen la comunicación, los cuales se pueden presentar en tiempo real. Párrafo reformado DOF 17-06-2016 La solicitud deberá ser resuelta por la autoridad judicial de manera inmediata, por cualquier medio que garantice su autenticidad, o en audiencia privada con la sola comparecencia del Ministerio Público, en un plazo que no exceda de las seis horas siguientes a que la haya recibido. También se requerirá autorización judicial en los casos de extracción de información, la cual consiste en la obtención de comunicaciones privadas, datos de identificación de las comunicaciones; así como la información, documentos, archivos de texto, audio, imagen o video contenidos en cualquier dispositivo, accesorio, aparato electrónico, equipo informático, aparato de almacenamiento y todo aquello que pueda contener información, incluyendo la almacenada en las plataformas o centros de datos remotos vinculados con éstos. Párrafo adicionado DOF 17-06-2016 Si la resolución se registra por medios diversos al escrito, los puntos resolutivos de la autorización deberán transcribirse y entregarse al Ministerio Público. Los servidores públicos autorizados para la ejecución de la medida serán responsables de que se realice en los términos de la resolución judicial. **Artículo 292. Requisitos de la solicitud:** La solicitud de intervención deberá estar fundada y motivada, precisar la persona o personas que serán sujetas a la

Nº	Medidas de investigación	Regulación de medidas de investigación en México
		medida; la identificación del lugar o lugares donde se realizará, si fuere posible; el tipo de comunicación a ser intervenida; su duración; el proceso que se llevará a cabo y las líneas, números o aparatos que serán intervenidos, y en su caso, la denominación de la empresa concesionada del servicio de telecomunicaciones a través del cual se realiza la comunicación objeto de la intervención. El plazo de la intervención, incluyendo sus prórrogas, no podrá exceder de seis meses. Después de dicho plazo, sólo podrán autorizarse nuevas intervenciones cuando el Ministerio Público acredite nuevos elementos que así lo justifiquen. **Artículo 294. Objeto de la intervención:** Podrán ser objeto de intervención las comunicaciones privadas que se realicen de forma oral, escrita, por signos, señales o mediante el empleo de aparatos eléctricos, electrónicos, mecánicos, alámbricos o inalámbricos, sistemas o equipos informáticos, así como por cualquier otro medio o forma que permita la comunicación entre uno o varios emisores y uno o varios receptores. En ningún caso se podrán autorizar intervenciones cuando se trate de materias de carácter electoral, fiscal, mercantil, civil, laboral o administrativo, ni en el caso de las comunicaciones del detenido con su Defensor. El Juez podrá en cualquier momento verificar que las intervenciones sean realizadas en los términos autorizados y, en caso de incumplimiento, decretar su revocación parcial o total.
5	Recogida en tiempo real de datos de tráfico (Artículo 20 Convenio de Budapest)	**Artículo 303. Localización geográfica en tiempo real y solicitud de entrega de datos conservados:** Cuando el Ministerio Público considere necesaria la localización geográfica en tiempo real o entrega de datos conservados por los concesionarios de telecomunicaciones, los autorizados o proveedores de servicios de aplicaciones y contenidos de los equipos de comunicación móvil asociados a una línea que se encuentra relacionada con los hechos que se investigan, el Procurador, o el servidor público en quien se delegue la facultad, podrá solicitar al Juez de control del fuero correspondiente en su caso, por cualquier medio, requiera a los concesionarios de telecomunicaciones, los autorizados o proveedores de servicios de aplicaciones y contenidos, para que proporcionen con la oportunidad y suficiencia necesaria a la autoridad investigadora, la información solicitada para el inmediato desahogo de dichos actos de investigación. Los datos conservados a que refiere este párrafo se destruirán en caso de que no constituyan medio de prueba idóneo o pertinente. En la solicitud se expresarán los equipos de comunicación móvil relacionados con los hechos que se investigan, señalando los motivos e indicios que sustentan la necesidad de la localización geográfica en tiempo real o la entrega de los datos conservados, su duración y, en su caso, la denominación de la empresa autorizada o proveedora del servicio de telecomunicaciones a través del cual se operan las líneas, números o aparatos que serán objeto de la medida. La petición deberá ser resuelta por la autoridad judicial de manera inmediata por cualquier medio que garantice su autenticidad, o en audiencia privada con la sola comparecencia del Ministerio Público. Si la resolución se emite o registra por medios diversos al escrito, los puntos resolutivos de la orden deberán transcribirse y entregarse al Ministerio Público.

Nº	Medidas de investigación	Regulación de medidas de investigación en México
		En caso de que el Juez de control niegue la orden de localización geográfica en tiempo real o la entrega de los datos conservados, el Ministerio Público podrá subsanar las deficiencias y solicitar nuevamente la orden o podrá apelar la decisión. En este caso la apelación debe ser resuelta en un plazo no mayor de doce horas a partir de que se interponga. Excepcionalmente, cuando esté en peligro la integridad física o la vida de una persona o se encuentre en riesgo el objeto del delito, así como en hechos relacionados con la privación ilegal de la libertad, secuestro, extorsión o delincuencia organizada, el Procurador, o el servidor público en quien se delegue la facultad, bajo su más estricta responsabilidad, ordenará directamente la localización geográfica en tiempo real o la entrega de los datos conservados a los concesionarios de telecomunicaciones, los autorizados o proveedores de servicios de aplicaciones y contenidos, quienes deberán atenderla de inmediato y con la suficiencia necesaria. A partir de que se haya cumplimentado el requerimiento, el Ministerio Público deberá informar al Juez de control competente por cualquier medio que garantice su autenticidad, dentro del plazo de cuarenta y ocho horas, a efecto de que ratifique parcial o totalmente de manera inmediata la subsistencia de la medida, sin perjuicio de que el Ministerio Público continúe con su actuación. Cuando el Juez de control no ratifique la medida a que hace referencia el párrafo anterior, la información obtenida no podrá ser incorporada al procedimiento penal. Asimismo el Procurador, o el servidor público en quien se delegue la facultad podrá requerir a los sujetos obligados que establece la Ley Federal de Telecomunicaciones y Radiodifusión, la conservación inmediata de datos contenidos en redes, sistemas o equipos de informática, hasta por un tiempo máximo de noventa días, lo cual deberá realizarse de forma inmediata. La solicitud y entrega de los datos contenidos en redes, sistemas o equipos de informática se llevará a cabo de conformidad por lo previsto por este artículo. Lo anterior sin menoscabo de las obligaciones previstas en materia de conservación de información para las concesionarias y autorizados de telecomunicaciones en términos del artículo 190, fracción II de la Ley Federal de Telecomunicaciones y Radiodifusión. Artículo reformado DOF 17-06-2016
6	Interceptación de datos relativos al contenido (Artículo 21 Convenio de Budapest)	**Artículo 291. Intervención de las comunicaciones privadas:** Cuando en la investigación el Ministerio Público considere necesaria la intervención de comunicaciones privadas, el Titular de la Procuraduría General de la República, o en quienes éste delegue esta facultad, así como los Procuradores de las entidades federativas, podrán solicitar al Juez federal de control competente, por cualquier medio, la autorización para practicar la intervención, expresando el objeto y necesidad de la misma. *Párrafo reformado DOF 17-06-2016* La intervención de comunicaciones privadas, abarca todo sistema de comunicación, o programas que sean resultado de la evolución tecnológica, que permitan el intercambio de datos, informaciones, audio, video, mensajes, así como archivos electrónicos que graben, conserven el contenido de las conversaciones o registren datos que identifiquen la comunicación, los cuales se

Nº	Medidas de investigación	Regulación de medidas de investigación en México
		pueden presentar en tiempo real. *Párrafo reformado DOF 17-06-2016* La solicitud deberá ser resuelta por la autoridad judicial de manera inmediata, por cualquier medio que garantice su autenticidad, o en audiencia privada con la sola comparecencia del Ministerio Público, en un plazo que no exceda de las seis horas siguientes a que la haya recibido. También se requerirá autorización judicial en los casos de extracción de información, la cual consiste en la obtención de comunicaciones privadas, datos de identificación de las comunicaciones; así como la información, documentos, archivos de texto, audio, imagen o video contenidos en cualquier dispositivo, accesorio, aparato electrónico, equipo informático, aparato de almacenamiento y todo aquello que pueda contener información, incluyendo la almacenada en las plataformas o centros de datos remotos vinculados con éstos. *Párrafo adicionado DOF 17-06-2016* Si la resolución se registra por medios diversos al escrito, los puntos resolutivos de la autorización deberán transcribirse y entregarse al Ministerio Público. Los servidores públicos autorizados para la ejecución de la medida serán responsables de que se realice en los términos de la resolución judicial. **Artículo 292. Requisitos de la solicitud:** La solicitud de intervención deberá estar fundada y motivada, precisar la persona o personas que serán sujetas a la medida; la identificación del lugar o lugares donde se realizará, si fuere posible; el tipo de comunicación a ser intervenida; su duración; el proceso que se llevará a cabo y las líneas, números o aparatos que serán intervenidos, y en su caso, la denominación de la empresa concesionada del servicio de telecomunicaciones a través del cual se realiza la comunicación objeto de la intervención. El plazo de la intervención, incluyendo sus prórrogas, no podrá exceder de seis meses. Después de dicho plazo, sólo podrán autorizarse nuevas intervenciones cuando el Ministerio Público acredite nuevos elementos que así lo justifiquen. **Artículo 294. Objeto de la intervención:** Podrán ser objeto de intervención las comunicaciones privadas que se realicen de forma oral, escrita, por signos, señales o mediante el empleo de aparatos eléctricos, electrónicos, mecánicos, alámbricos o inalámbricos, sistemas o equipos informáticos, así como por cualquier otro medio o forma que permita la comunicación entre uno o varios emisores y uno o varios receptores. En ningún caso se podrán autorizar intervenciones cuando se trate de materias de carácter electoral, fiscal, mercantil, civil, laboral o administrativo, ni en el caso de las comunicaciones del detenido con su Defensor. El Juez podrá en cualquier momento verificar que las intervenciones sean realizadas en los términos autorizados y, en caso de incumplimiento, decretar su revocación parcial o total.
7	Agente encubierto digital	**No se encontró medida especial aplicable.**
8	Registro remoto	**No se encontró medida especial aplicable.**
9	OSINT	**No se encontró medida especial aplicable.**

Nº	Medidas de investigación	Regulación de medidas de investigación en México
10	Acceso transfronterizo de datos	**No se encontró medida especial aplicable.**
11	Hallazgos casuales en evidencia digital	**Artículo 295. Conocimiento de delito diverso:** Si en la práctica de una intervención de comunicaciones privadas se tuviera conocimiento de la comisión de un delito diverso de aquellos que motivan la medida, se hará constar esta circunstancia en el registro para dar inicio a una nueva investigación.
12	Desbloqueo compulsivo de datos informáticos	**No se encontró medida especial aplicable.**

Tabla Nº 32: Resumen de medidas de investigación reguladas en México

7.5.3. Conservación de comunicaciones

Debemos comenzar haciendo una referencia a la Ley Federal de Telecomunicaciones y Radiodifusión Mexicana[534], donde en el título octavo "De la Colaboración con la Justicia", el artículo 190 establece que los concesionarios de telecomunicaciones deberán colaborar con las instancias de seguridad, procuración y administración de justicia, en la localización geográfica, en tiempo real, de los equipos de comunicación móvil, en los términos que establezcan las leyes.

En el inc. 2 del precitado artículo, establece la obligación de "*conservar un registro y control de comunicaciones que se realicen desde cualquier tipo de línea que utilice numeración propia o arrendada, bajo cualquier modalidad, que permitan identificar con precisión los siguientes datos:*

a) Nombre, denominación o razón social y domicilio del suscriptor;

b) Tipo de comunicación (transmisión de voz, buzón vocal, conferencia, datos), servicios suplementarios (incluidos el reenvío o transferencia de llamada) o servicios de mensajería o multimedia empleados (incluidos los servicios de mensajes cortos, servicios multimedia y avanzados);

[534] CÁMARA DE DIPUTADOS DEL HONORABLE CONGRESO DE LA UNIÓN, Ley Federal de Telecomunicaciones y Radiodifusión; Disponible en: https://www.diputados.gob.mx/LeyesBiblio/pdf/LFTR.pdf

c) Datos necesarios para rastrear e identificar el origen y destino de las comunicaciones de telefonía móvil: número de destino, modalidad de líneas con contrato o plan tarifario, como en la modalidad de líneas de prepago;

d) Datos necesarios para determinar la fecha, hora y duración de la comunicación, así como el servicio de mensajería o multimedia;

e) Además de los datos anteriores, se deberá conservar la fecha y hora de la primera activación del servicio y la etiqueta de localización (identificador de celda) desde la que se haya activado el servicio;

f) En su caso, identificación y características técnicas de los dispositivos, incluyendo, entre otros, los códigos internacionales de identidad de fabricación del equipo y del suscriptor;

g) La ubicación digital del posicionamiento geográfico de las líneas telefónicas, y

h) La obligación de conservación de datos, comenzará a contarse a partir de la fecha en que se haya producido la comunicación."

En cuanto al tema de los plazos, se define que se deberá conservar los datos referidos en el párrafo anterior durante los primeros doce meses en sistemas que permitan su consulta y entrega en tiempo real a las autoridades competentes, a través de medios electrónicos. Concluido el plazo referido, el concesionario deberá conservar dichos datos por doce meses adicionales en sistemas de almacenamiento electrónico, en cuyo caso, la entrega de la información a las autoridades competentes se realizará dentro de las cuarenta y ocho horas siguientes, contadas a partir de la notificación de la solicitud.

Si bien continúa la regulación, es suficiente referencia, toda vez que en la parte final del artículo 303 del Código Nacional de Procedimientos Penales Mexicano, establece que el Procurador podrá requerir a los sujetos obligados por la Ley Federal de Telecomunicaciones y Radiodifusión, la conservación inmediata de datos contenidos en redes, sistemas o equipos de informática, hasta por un tiempo máximo de noventa días, lo cual deberá realizarse de forma inmediata.

Adicionalmente, se regula que tanto la solicitud como la entrega de los datos contenidos en redes, sistemas o equipos de informática se llevará a cabo de conformidad por lo previsto por el artículo 303, que como veremos más adelante al analizar la medida de localización geográfica, establece algunos requisitos legales para su acceso.

7.5.4. Colaboración con la autoridad y aporte voluntario

Si bien no hemos identificado la existencia de un artículo particular que haga referencia a la posibilidad del mandato de comunicación, hemos considerado como parcialmente aplicable a forma de reemplazo de dicha medida, la combinación entre los artículos 276 y 301.

Por una parte, el art. 276 regula la aportación de comunicaciones entre particulares, como una forma alternativa de incorporación de prueba al proceso penal, cuando hayan sido obtenidas directamente por alguno de los participantes en la misma.

El artículo establece que (en cumplimiento del principio de relevancia) las comunicaciones aportadas por los particulares deberán estar estrechamente vinculadas con el delito que se investiga, por lo que en ningún caso el juez admitirá comunicaciones que violen el deber de confidencialidad.

Por otro lado, el artículo 301, más relacionado con el mandato de comunicación, establece que los concesionarios, permisionarios y demás titulares de los medios o sistemas susceptibles de intervención, deberán colaborar eficientemente con la autoridad competente para cumplir con los actos de investigación.

El segundo párrafo, establece la obligación para las empresas en relación a que deberán contar con la capacidad técnica indispensable que atienda las exigencias requeridas por la autoridad judicial para operar una orden de intervención de comunicaciones privadas, dejando abierta la posibilidad de sanción en caso de incumplimiento.

7.5.5. Intervención de comunicaciones y extracción de información

El artículo 291 establece la posibilidad para que tanto el Ministerio Público así como los Procuradores de las entidades federativas, puedan solicitar al Juez federal de control competente, por cualquier medio, la autorización para practicar la intervención, expresando el objeto y necesidad de la misma.

En el año 2016, se modificó el segundo párrafo, agregándose una explicación acerca que comunicaciones privadas abarca todo sistema de comunicación, o programas que sean resultado de la evolución tecnológica, que permitan el intercambio de datos, informaciones, audio, video, mensajes, así como archivos electrónicos que graben, conserven el contenido de las conversaciones o registren datos que identifiquen la comunicación, los cuales se pueden presentar en tiempo real.

El artículo establece que esta medida de investigación, en consonancia con el respeto por la privacidad de las personas, deberá ser autorizada por la autoridad judicial, en un plazo que no exceda de las seis horas siguientes a que la haya recibido.

La razón por la que hemos considerado que este artículo cumple -al menos parcialmente- con la medida de registro y decomiso de datos informáticos almacenados, tiene que ver con la segunda parte del mismo artículo, donde se establece que "*También se requerirá autorización judicial en los casos de extracción de información, la cual consiste en la obtención de comunicaciones privadas, datos de identificación de las comunicaciones; así como la información, documentos, archivos de texto, audio, imagen o video contenidos en cualquier dispositivo, accesorio, aparato electrónico, equipo informático, aparato de almacenamiento y todo aquello que pueda contener información, incluyendo la almacenada en las plataformas o centros de datos remotos vinculados con éstos*".

Por otro lado, el art. 292 establece que la solicitud de intervención deberá estar fundada y motivada, precisar la persona o personas que serán sujetas a la medida; la identificación del lugar o lugares donde se realizará, si fuere posible; el tipo de comunicación a ser intervenida; su duración; el proceso que se llevará a cabo y las líneas, números o aparatos que serán intervenidos, y en su caso, la denominación de la empresa concesionada del servicio de telecomunicaciones a través del cual se realiza la comunicación objeto de la intervención.

Entre los límites definidos, puede observarse que el plazo de la intervención, incluyendo sus prórrogas, no podrá exceder de seis meses.

Finalmente, hemos incluído el art. 294 toda vez que establece que podrá ser objeto de intervención las comunicaciones privadas que se realicen de forma oral, escrita, por signos, señales o mediante el empleo de aparatos eléctricos, electrónicos, mecánicos, alámbricos o inalámbricos, sistemas o equipos informáticos, así como por cualquier otro medio o forma que permita la comunicación entre uno o varios emisores y uno o varios receptores.

Una interpretación amplia del artículo anterior, podría considerar que la intervención de un equipo o sistema informático, implicaría la autorización de la medida del registro remoto. En nuestro caso, no hemos considerado tal cosa, toda vez que entendemos que habilitar una medida de investigación tan gravosa como el allanamiento o registro remoto, requiere de un artículo específico que la regule, tal como hemos visto en el caso de la Provincia de Neuquén o Salta, en Argentina.

Otra limitación que se destaca, es que en ningún caso se podrán autorizar intervenciones cuando se trate de materias de carácter electoral, fiscal, mercantil, civil, laboral o administrativo, ni en el caso de las comunicaciones del detenido con su defensor.

7.5.6. Localización geográfica en tiempo real

Una novedad que hemos encontrado en el sistema procesal penal mexicano a través del art. 3030 que consiste en la inclusión de una medida que posibilita al

Ministerio Público acceder a la localización geográfica en tiempo real o a la entrega de datos conservados por un proveedor de servicios.

Dicha medida debe ser solicitada al Juez de control del fuero correspondiente, para que se requiera a los proveedores de servicios de telecomunicaciones la información que se considere de interés para la investigación en curso.

En la solicitud debe especificarse: los equipos de comunicación móvil relacionados con los hechos que se investigan; los motivos e indicios que sustentan la necesidad de la localización geográfica en tiempo real o la entrega de los datos conservados; su duración y; en su caso, la denominación de la empresa autorizada o proveedora del servicio de telecomunicaciones a través del cual se operan las líneas; números o aparatos que serán objeto de la medida.

La regulación mexicana trae un caso de excepción a la regla antes comentada, y será para cuando esté en peligro la integridad física o la vida de una persona o se encuentre en riesgo el objeto del delito, así como en hechos relacionados con la privación ilegal de la libertad, secuestro, extorsión o delincuencia organizada. En estos casos, el Procurador podrá ordenar de forma directa la localización geográfica en tiempo real o la entrega de los datos conservados a los proveedores de servicios de telecomunicaciones. Luego de ejecutada la medida, el Ministerio Público deberá informar al Juez de control competente por cualquier medio que garantice su autenticidad, dentro del plazo de cuarenta y ocho horas, a efecto de que ratifique parcial o totalmente de manera inmediata la subsistencia de la medida, sin perjuicio de que el Ministerio Público continúe con su actuación.

En caso que el Juez de control no ratifique la medida a que hace referencia el párrafo anterior, la información obtenida no podrá ser incorporada al procedimiento penal.

7.6. Medidas de investigación reguladas en España

7.6.1. La Ley de Enjuiciamiento Criminal española

A las dificultades propias de la investigación tecnológica de los delitos informáticos, España le sumaba tener una legislación vigente, su Ley de Enjuiciamiento Criminal (en adelante LECrim) de 1882 muy parcheada para intentar hacer frente a los nuevos retos, se encontraba anticuada y por ello no se adaptaba a las nuevas necesidades de la investigación criminal por lo que exigía de los jueces y magistrados una gran labor jurisprudencial para suplir los vacíos legales existentes.

Dada esta situación era necesaria una reforma de la LECrim que contemplara este nuevo tipo de delincuencia y se adaptara a la nueva realidad social. La reforma a la que nos vamos a referir en este breve artículo tuvo su origen el 5 de Diciembre de 2014 con la aprobación, por el Consejo de Ministros, de un Anteproyecto de Ley Orgánica de modificación de la LECrim para la agilización de la justicia penal, el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológicas.

En su Exposición de Motivos se ponía de manifiesto la necesidad de afrontar ciertas cuestiones que no podían esperar a ser resueltas con la promulgación de un nuevo texto normativo que sustituyera a la Ley de Enjuiciamiento Criminal. Dichas cuestiones eran: 1) la necesidad de establecer disposiciones eficaces de agilización de la justicia penal que eviten dilaciones indebidas; 2) el fortalecimiento de los derechos procesales de conformidad con la exigencias del Derecho de la Unión Europea (UE); 3) la regulación de las medidas de investigación tecnológica; 4) la previsión de un procedimiento de decomiso autónomo; 5) la instauración de la segunda instancia; y, 6) la reforma de la revisión penal.

Este Anteproyecto de Ley Orgánica se dividió posteriormente en dos proyectos de ley: el Proyecto de Ley de modificación de la LECrim para la agilización de la justicia penal y el fortalecimiento de las garantías procesales, y el Proyecto de Ley Orgánica de modificación de la LECrim para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica. Casi un año

más tarde se promulgó la Ley Orgánica 13/2015, de 5 de Octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica y la Ley 41/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para la agilización de la justicia penal y el fortalecimiento de las garantías procesales.

Particularmente para nuestro caso de estudio, realizaremos un relevamiento de las medidas de investigación incorporadas a partir de las reformas que introduce la Ley Orgánica 13/2015 de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, concretamente en este último aspecto, es decir, para mejorar las medidas de investigación criminal tecnológica en el ámbito de derechos a la intimidad, al secreto de las comunicaciones y a la protección de datos personales garantizados en el artículo 18[535] de la Constitución Nacional Española.

7.6.2. Cuadro de medidas de investigación reguladas

Nº	Medidas de investigación	Regulación de medidas de investigación en España
1	Conservación inmediata de datos informáticos almacenados (Artículo 16 Convenio de Budapest)	**Artículo 588 octies. Orden de conservación de datos.** El Ministerio Fiscal o la Policía Judicial podrán requerir a cualquier persona física o jurídica la conservación y protección de datos o informaciones concretas incluidas en un sistema informático de almacenamiento que se encuentren a su disposición hasta que se obtenga la autorización judicial correspondiente para su cesión con arreglo a lo dispuesto en los artículos precedentes. Los datos se conservarán durante un periodo máximo de noventa días, prorrogable una sola vez hasta que se autorice la cesión o se cumplan ciento ochenta días.
2	Conservación y divulgación inmediata de los datos de tráfico (Artículo 17 Convenio de	**Artículo 588 octies. Orden de conservación de datos.** El Ministerio Fiscal o la Policía Judicial podrán requerir a cualquier persona física o jurídica la conservación y protección de datos o informaciones concretas incluidas en un sistema informático de almacenamiento que se encuentren a su disposición hasta que se obtenga la autorización judicial correspondiente para su cesión con arreglo a lo dispuesto en los artículos precedentes. Los datos se conservarán durante un periodo máximo de noventa días,

[535] Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen. 2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito.

Nº	Medidas de investigación	Regulación de medidas de investigación en España
	Budapest)	prorrogable una sola vez hasta que se autorice la cesión o se cumplan ciento ochenta días.
3	Mandato de comunicación (Artículo 18 Convenio de Budapest)	**Sección 3.ª Acceso a los datos necesarios para la identificación de usuarios, terminales y dispositivos de conectividad** **Artículo 588 ter k. Identificación mediante número IP:** Cuando en el ejercicio de las funciones de prevención y descubrimiento de los delitos cometidos en internet, los agentes de la Policía Judicial tuvieran acceso a una dirección IP que estuviera siendo utilizada para la comisión algún delito y no constara la identificación y localización del equipo o del dispositivo de conectividad correspondiente ni los datos de identificación personal del usuario, solicitarán del juez de instrucción que requiera de los agentes sujetos al deber de colaboración según el artículo 588 ter e, la cesión de los datos que permitan la identificación y localización del terminal o del dispositivo de conectividad y la identificación del sospechoso. **Artículo 588 ter l. Identificación de los terminales mediante captación de códigos de identificación del aparato o de sus componentes:** 1. Siempre que en el marco de una investigación no hubiera sido posible obtener un determinado número de abonado y este resulte indispensable a los fines de la investigación, los agentes de Policía Judicial podrán valerse de artificios técnicos que permitan acceder al conocimiento de los códigos de identificación o etiquetas técnicas del aparato de telecomunicación o de alguno de sus componentes, tales como la numeración IMSI o IMEI y, en general, de cualquier medio técnico que, de acuerdo con el estado de la tecnología, sea apto para identificar el equipo de comunicación utilizado o la tarjeta utilizada para acceder a la red de telecomunicaciones. 2. Una vez obtenidos los códigos que permiten la identificación del aparato o de alguno de sus componentes, los agentes de la Policía Judicial podrán solicitar del juez competente la intervención de las comunicaciones en los términos establecidos en el artículo 588 ter d. La solicitud habrá de poner en conocimiento del órgano jurisdiccional la utilización de los artificios a que se refiere el apartado anterior. El tribunal dictará resolución motivada concediendo o denegando la solicitud de intervención en el plazo establecido en el artículo 588 bis c. **Artículo 588 ter m. Identificación de titulares o terminales o dispositivos de conectividad:** Cuando, en el ejercicio de sus funciones, el Ministerio Fiscal o la Policía Judicial necesiten conocer la titularidad de un número de teléfono o de cualquier otro medio de comunicación, o, en sentido inverso, precisen el número de teléfono o los datos identificativos de cualquier medio de comunicación, podrán dirigirse directamente a los prestadores de servicios de telecomunicaciones, de acceso a una red de telecomunicaciones o de servicios de la sociedad de la información, quienes estarán obligados a cumplir el requerimiento, bajo apercibimiento de incurrir en el delito de desobediencia.»
4	Registro y decomiso de datos informáticos	**Registro de dispositivos de almacenamiento masivo de información** **Artículo 588 sexies a. Necesidad de motivación individualizada: 1. Cuando con ocasión de la práctica de un registro domiciliario sea previsible la**

Nº	Medidas de investigación	Regulación de medidas de investigación en España
	almacenados (Artículo 19 Convenio de Budapest)	**aprehensión de ordenadores, instrumentos de comunicación telefónica** o telemática o dispositivos de almacenamiento masivo de información digital o el acceso a repositorios telemáticos de datos, la resolución del juez de instrucción habrá de extender su razonamiento a la justificación, en su caso, de las razones que legitiman el acceso de los agentes facultados a la información contenida en tales dispositivos. 2. La simple incautación de cualquiera de los dispositivos a los que se refiere el apartado anterior, practicada durante el transcurso de la diligencia de registro domiciliario, no legitima el acceso a su contenido, sin perjuicio de que dicho acceso pueda ser autorizado ulteriormente por el juez competente. **Artículo 588 sexies b. Acceso a la información de dispositivos electrónicos incautados fuera del domicilio del investigado:** La exigencia prevista en el apartado 1 del artículo anterior será también aplicable a aquellos casos en los que los ordenadores, instrumentos de comunicación o dispositivos de almacenamiento masivo de datos, o el acceso a repositorios telemáticos de datos, sean aprehendidos con independencia de un registro domiciliario. En tales casos, los agentes pondrán en conocimiento del juez la incautación de tales efectos. Si éste considera indispensable el acceso a la información albergada en su contenido, otorgará la correspondiente autorización. **Artículo 588 sexies c. Autorización judicial:** 1. La resolución del juez de instrucción mediante la que se autorice el acceso a la información contenida en los dispositivos a que se refiere la presente sección, fijará los términos y el alcance del registro y podrá autorizar la realización de copias de los datos informáticos. Fijará también las condiciones necesarias para asegurar la integridad de los datos y las garantías de su preservación para hacer posible, en su caso, la práctica de un dictamen pericial. 2. Salvo que constituyan el objeto o instrumento del delito o existan otras razones que lo justifiquen, se evitará la incautación de los soportes físicos que contengan los datos o archivos informáticos, cuando ello pueda causar un grave perjuicio a su titular o propietario y sea posible la obtención de una copia de ellos en condiciones que garanticen la autenticidad e integridad de los datos.
5	Recogida en tiempo real de datos de tráfico (Artículo 20 Convenio de Budapest)	**Artículo 588 ter j. Datos obrantes en archivos automatizados de los prestadores de servicios:** 1. Los datos electrónicos conservados por los prestadores de servicios o personas que faciliten la comunicación en cumplimiento de la legislación sobre retención de datos relativos a las comunicaciones electrónicas o por propia iniciativa por motivos comerciales o de otra índole y que se encuentren vinculados a procesos de comunicación, solo podrán ser cedidos para su incorporación al proceso con autorización judicial. 2. Cuando el conocimiento de esos datos resulte indispensable para la investigación, se solicitará del juez competente autorización para recabar la información que conste en los archivos automatizados de los prestadores de servicios, incluida la búsqueda entrecruzada o inteligente de datos, siempre que se precisen la naturaleza de los datos que hayan de ser conocidos y las razones que justifican la cesión.
6	Interceptación de	**Artículo 588 ter a. Presupuestos:** La autorización para la interceptación de las

Nº	Medidas de investigación	Regulación de medidas de investigación en España
	datos relativos al contenido (Artículo 21 Convenio de Budapest)	comunicaciones telefónicas y telemáticas solo podrá ser concedida cuando la investigación tenga por objeto alguno de los delitos a que se refiere el artículo 579.1 de esta ley o delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la comunicación o servicio de comunicación. **Artículo 588 ter b. Ámbito:** 1. Los terminales o medios de comunicación objeto de intervención han de ser aquellos habitual u ocasionalmente utilizados por el investigado. 2. La intervención judicialmente acordada podrá autorizar el acceso al contenido de las comunicaciones y a los datos electrónicos de tráfico o asociados al proceso de comunicación, así como a los que se produzcan con independencia del establecimiento o no de una concreta comunicación, en los que participe el sujeto investigado, ya sea como emisor o como receptor, y podrá afectar a los terminales o los medios de comunicación de los que el investigado sea titular o usuario. También podrán intervenirse los terminales o medios de comunicación de la víctima cuando sea previsible un grave riesgo para su vida o integridad. A los efectos previstos en este artículo, se entenderá por datos electrónicos de tráfico o asociados todos aquellos que se generan como consecuencia de la conducción de la comunicación a través de una red de comunicaciones electrónicas, de su puesta a disposición del usuario, así como de la prestación de un servicio de la sociedad de la información o comunicación telemática de naturaleza análoga. **Artículo 588 ter c. Afectación a tercero:** Podrá acordarse la intervención judicial de las comunicaciones emitidas desde terminales o medios de comunicación telemática pertenecientes a una tercera persona siempre que: 1.º exista constancia de que el sujeto investigado se sirve de aquella para transmitir o recibir información, o 2.º el titular colabore con la persona investigada en sus fines ilícitos o se beneficie de su actividad. También podrá autorizarse dicha intervención cuando el dispositivo objeto de investigación sea utilizado maliciosamente por terceros por vía telemática, sin conocimiento de su titular. **Artículo 588 ter d. Solicitud de autorización judicial:** 1. La solicitud de autorización judicial deberá contener, además de los requisitos mencionados en el artículo 588 bis b, los siguientes: a) la identificación del número de abonado, del terminal o de la etiqueta técnica, b) la identificación de la conexión objeto de la intervención o c) los datos necesarios para identificar el medio de telecomunicación de que se trate. 2. Para determinar la extensión de la medida, la solicitud de autorización judicial podrá tener por objeto alguno de los siguientes extremos: a) El registro y la grabación del contenido de la comunicación, con indicación de la forma o tipo de comunicaciones a las que afecta. b) El conocimiento de su origen o destino, en el momento en el que la comunicación se realiza.

Nº	Medidas de investigación	Regulación de medidas de investigación en España
		c) La localización geográfica del origen o destino de la comunicación. d) El conocimiento de otros datos de tráfico asociados o no asociados pero de valor añadido a la comunicación. En este caso, la solicitud especificará los datos concretos que han de ser obtenidos. 3. En caso de urgencia, cuando las investigaciones se realicen para la averiguación de delitos relacionados con la actuación de bandas armadas o elementos terroristas y existan razones fundadas que hagan imprescindible la medida prevista en los apartados anteriores de este artículo, podrá ordenarla el Ministro del Interior o, en su defecto, el Secretario de Estado de Seguridad. Esta medida se comunicará inmediatamente al juez competente y, en todo caso, dentro del plazo máximo de veinticuatro horas, haciendo constar las razones que justificaron la adopción de la medida, la actuación realizada, la forma en que se ha efectuado y su resultado. El juez competente, también de forma motivada, revocará o confirmará tal actuación en un plazo máximo de setenta y dos horas desde que fue ordenada la medida. **Artículo 588 ter e. Deber de colaboración:** 1. Todos los prestadores de servicios de telecomunicaciones, de acceso a una red de telecomunicaciones o de servicios de la sociedad de la información, así como toda persona que de cualquier modo contribuya a facilitar las comunicaciones a través del teléfono o de cualquier otro medio o sistema de comunicación telemática, lógica o virtual, están obligados a prestar al juez, al Ministerio Fiscal y a los agentes de la Policía Judicial designados para la práctica de la medida la asistencia y colaboración precisas para facilitar el cumplimiento de los autos de intervención de las telecomunicaciones. 2. Los sujetos requeridos para prestar colaboración tendrán la obligación de guardar secreto acerca de las actividades requeridas por las autoridades. 3. Los sujetos obligados que incumplieren los anteriores deberes podrán incurrir en delito de desobediencia. **Artículo 588 ter f. Control de la medida:** En cumplimiento de lo dispuesto en el artículo 588 bis g, la Policía Judicial pondrá a disposición del juez, con la periodicidad que este determine y en soportes digitales distintos, la transcripción de los pasajes que considere de interés y las grabaciones íntegras realizadas. Se indicará el origen y destino de cada una de ellas y se asegurará, mediante un sistema de sellado o firma electrónica avanzado o sistema de adveración suficientemente fiable, la autenticidad e integridad de la información volcada desde el ordenador central a los soportes digitales en que las comunicaciones hubieran sido grabadas. **Artículo 588 ter g. Duración:** La duración máxima inicial de la intervención, que se computará desde la fecha de autorización judicial, será de tres meses, prorrogables por períodos sucesivos de igual duración hasta el plazo máximo de dieciocho meses. **Artículo 588 ter h. Solicitud de prórroga:** Para la fundamentación de la solicitud de la prórroga, la Policía Judicial aportará, en su caso, la transcripción de aquellos pasajes de las conversaciones de las que se deduzcan informaciones relevantes para decidir sobre el mantenimiento de la medida.

Nº	Medidas de investigación	Regulación de medidas de investigación en España
		Antes de dictar la resolución, el juez podrá solicitar aclaraciones o mayor información, incluido el contenido íntegro de las conversaciones intervenidas. **Artículo 588 ter i. Acceso de las partes a las grabaciones:** 1. Alzado el secreto y expirada la vigencia de la medida de intervención, se entregará a las partes copia de las grabaciones y de las transcripciones realizadas. Si en la grabación hubiera datos referidos a aspectos de la vida íntima de las personas, solo se entregará la grabación y transcripción de aquellas partes que no se refieran a ellos. La no inclusión de la totalidad de la grabación en la transcripción entregada se hará constar de modo expreso. 2. Una vez examinadas las grabaciones y en el plazo fijado por el juez, en atención al volumen de la información contenida en los soportes, cualquiera de las partes podrá solicitar la inclusión en las copias de aquellas comunicaciones que entienda relevantes y hayan sido excluidas. El juez de instrucción, oídas o examinadas por sí esas comunicaciones, decidirá sobre su exclusión o incorporación a la causa. 3. Se notificará por el juez de instrucción a las personas intervinientes en las comunicaciones interceptadas el hecho de la práctica de la injerencia y se les informará de las concretas comunicaciones en las que haya participado que resulten afectadas, salvo que sea imposible, exija un esfuerzo desproporcionado o puedan perjudicar futuras investigaciones. Si la persona notificada lo solicita se le entregará copia de la grabación o transcripción de tales comunicaciones, en la medida que esto no afecte al derecho a la intimidad de otras personas o resulte contrario a los fines del proceso en cuyo marco se hubiere adoptado la medida de injerencia. **Artículo 588 quater a. Grabación de las comunicaciones orales directas:** 1. Podrá autorizarse la colocación y utilización de dispositivos electrónicos que permitan la captación y grabación de las comunicaciones orales directas que se mantengan por el investigado, en la vía pública o en otro espacio abierto, en su domicilio o en cualesquiera otros lugares cerrados. Los dispositivos de escucha y grabación podrán ser colocados tanto en el exterior como en el interior del domicilio o lugar cerrado. 2. En el supuesto en que fuera necesaria la entrada en el domicilio o en alguno de los espacios destinados al ejercicio de la privacidad, la resolución habilitante habrá de extender su motivación a la procedencia del acceso a dichos lugares. 3. La escucha y grabación de las conversaciones privadas se podrá complementar con la obtención de imágenes cuando expresamente lo autorice la resolución judicial que la acuerde.
7	Agente encubierto digital	**Artículo 282 bis:** 1. A los fines previstos en el artículo anterior y cuando se trate de investigaciones que afecten a actividades propias de la delincuencia organizada, el Juez de Instrucción competente o el Ministerio Fiscal dando cuenta inmediata al Juez, podrán autorizar a funcionarios de la Policía Judicial, mediante resolución fundada y teniendo en cuenta su necesidad a los fines de la investigación, a actuar bajo identidad supuesta y a adquirir y transportar los objetos, efectos e instrumentos del delito y diferir la incautación de los mismos. La identidad supuesta será otorgada por el Ministerio del Interior por el plazo de seis meses prorrogables por períodos de igual duración, quedando

Nº	Medidas de investigación	Regulación de medidas de investigación en España
		legítimamente habilitados para actuar en todo lo relacionado con la investigación concreta y a participar en el tráfico jurídico y social bajo tal identidad. La resolución por la que se acuerde deberá consignar el nombre verdadero del agente y la identidad supuesta con la que actuará en el caso concreto. La resolución será reservada y deberá conservarse fuera de las actuaciones con la debida seguridad. La información que vaya obteniendo el agente encubierto deberá ser puesta a la mayor brevedad posible en conocimiento de quien autorizó la investigación. Asimismo, dicha información deberá aportarse al proceso en su integridad y se valorará en conciencia por el órgano judicial competente. 2. Los funcionarios de la Policía Judicial que hubieran actuado en una investigación con identidad falsa de conformidad a lo previsto en el apartado 1, podrán mantener dicha identidad cuando testifiquen en el proceso que pudiera derivarse de los hechos en que hubieran intervenido y siempre que así se acuerde mediante resolución judicial motivada, siéndole también de aplicación lo previsto en la Ley Orgánica 19/1994, de 23 de diciembre. Ningún funcionario de la Policía Judicial podrá ser obligado a actuar como agente encubierto. 3. Cuando las actuaciones de investigación puedan afectar a los derechos fundamentales, el agente encubierto deberá solicitar del órgano judicial competente las autorizaciones que, al respecto, establezca la Constitución y la Ley, así como cumplir las demás previsiones legales aplicables. 4. A los efectos señalados en el apartado 1 de este artículo, se considerará como delincuencia organizada la asociación de tres o más personas para realizar, de forma permanente o reiterada, conductas que tengan como fin cometer alguno o algunos de los delitos siguientes: a) Delitos de obtención, tráfico ilícito de órganos humanos y trasplante de los mismos, previstos en el artículo 156 bis del Código Penal. b) Delito de secuestro de personas previsto en los artículos 164 a 166 del Código Penal. c) Delito de trata de seres humanos previsto en el artículo 177 bis del Código Penal. d) Delitos relativos a la prostitución previstos en los artículos 187 a 189 del Código Penal. e) Delitos contra el patrimonio y contra el orden socioeconómico previstos en los artículos 237, 243, 244, 248 y 301 del Código Penal. f) Delitos relativos a la propiedad intelectual e industrial previstos en los artículos 270 a 277 del Código Penal. g) Delitos contra los derechos de los trabajadores previstos en los artículos 312 y 313 del Código Penal. h) Delitos contra los derechos de los ciudadanos extranjeros previstos en el artículo 318 bis del Código Penal. i) Delitos de tráfico de especies de flora o fauna amenazada previstos en los artículos 332 y 334 del Código Penal. j) Delito de tráfico de material nuclear y radiactivo previsto en el artículo 345 del Código Penal. k) Delitos contra la salud pública previstos en los artículos 368 a 373 del Código Penal. l) Delitos de falsificación de moneda, previsto en el artículo 386 del Código

Nº	Medidas de investigación	Regulación de medidas de investigación en España
		Penal, y de falsificación de tarjetas de crédito o débito o cheques de viaje, previsto en el artículo 399 bis del Código Penal. m) Delito de tráfico y depósito de armas, municiones o explosivos previsto en los artículos 566 a 568 del Código Penal. n) Delitos de terrorismo previstos en los artículos 572 a 578 del Código Penal. o) Delitos contra el patrimonio histórico previstos en el artículo 2.1.e de la Ley Orgánica 12/1995, de 12 de diciembre, de represión del contrabando. 5. El agente encubierto estará exento de responsabilidad criminal por aquellas actuaciones que sean consecuencia necesaria del desarrollo de la investigación, siempre que guarden la debida proporcionalidad con la finalidad de la misma y no constituyan una provocación al delito. Para poder proceder penalmente contra el mismo por las actuaciones realizadas a los fines de la investigación, el Juez competente para conocer la causa deberá, tan pronto tenga conocimiento de la actuación de algún agente encubierto en la misma, requerir informe relativo a tal circunstancia de quien hubiere autorizado la identidad supuesta, en atención al cual resolverá lo que a su criterio proceda. 6. El juez de instrucción podrá autorizar a funcionarios de la Policía Judicial para actuar bajo identidad supuesta en comunicaciones mantenidas en canales cerrados de comunicación con el fin de esclarecer alguno de los delitos a los que se refiere el apartado 4 de este artículo o cualquier delito de los previstos en el artículo 588 ter a. El agente encubierto informático, con autorización específica para ello, podrá intercambiar o enviar por sí mismo archivos ilícitos por razón de su contenido y analizar los resultados de los algoritmos aplicados para la identificación de dichos archivos ilícitos. 7. En el curso de una investigación llevada a cabo mediante agente encubierto, el juez competente podrá autorizar la obtención de imágenes y la grabación de las conversaciones que puedan mantenerse en los encuentros previstos entre el agente y el investigado, aun cuando se desarrollen en el interior de un domicilio.
8	Registro remoto	**Registros remotos sobre equipos informáticos** **Artículo 588 septies a. Presupuestos:** 1. El juez competente podrá autorizar la utilización de datos de identificación y códigos, así como la instalación de un software, que permitan, de forma remota y telemática, el examen a distancia y sin conocimiento de su titular o usuario del contenido de un ordenador, dispositivo electrónico, sistema informático, instrumento de almacenamiento masivo de datos informáticos o base de datos, siempre que persiga la investigación de alguno de los siguientes delitos: a) Delitos cometidos en el seno de organizaciones criminales. b) Delitos de terrorismo. c) Delitos cometidos contra menores o personas con capacidad modificada judicialmente. d) Delitos contra la Constitución, de traición y relativos a la defensa nacional. e) Delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la telecomunicación o servicio de comunicación. 2. La resolución judicial que autorice el registro deberá especificar: a) Los ordenadores, dispositivos electrónicos, sistemas informáticos o parte de los mismos, medios informáticos de almacenamiento de datos o bases de datos,

Nº	Medidas de investigación	Regulación de medidas de investigación en España
		datos u otros contenidos digitales objeto de la medida. b) El alcance de la misma, la forma en la que se procederá al acceso y aprehensión de los datos o archivos informáticos relevantes para la causa y el software mediante el que se ejecutará el control de la información. c) Los agentes autorizados para la ejecución de la medida. d) La autorización, en su caso, para la realización y conservación de copias de los datos informáticos. e) Las medidas precisas para la preservación de la integridad de los datos almacenados, así como para la inaccesibilidad o supresión de dichos datos del sistema informático al que se ha tenido acceso. 3. Cuando los agentes que lleven a cabo el registro remoto tengan razones para creer que los datos buscados están almacenados en otro sistema informático o en una parte del mismo, pondrán este hecho en conocimiento del juez, quien podrá autorizar una ampliación de los términos del registro. **Artículo 588 septies b. Deber de colaboración:** 1. Los prestadores de servicios y personas señaladas en el artículo 588 ter e y los titulares o responsables del sistema informático o base de datos objeto del registro están obligados a facilitar a los agentes investigadores la colaboración precisa para la práctica de la medida y el acceso al sistema. Asimismo, están obligados a facilitar la asistencia necesaria para que los datos e información recogidos puedan ser objeto de examen y visualización. 2. Las autoridades y los agentes encargados de la investigación podrán ordenar a cualquier persona que conozca el funcionamiento del sistema informático o las medidas aplicadas para proteger los datos informáticos contenidos en el mismo que facilite la información que resulte necesaria para el buen fin de la diligencia. Esta disposición no será aplicable al investigado o encausado, a las personas que están dispensadas de la obligación de declarar por razón de parentesco, y a aquellas que, de conformidad con el artículo 416.2, no pueden declarar en virtud del secreto profesional. 3. Los sujetos requeridos para prestar colaboración tendrán la obligación de guardar secreto acerca de las actividades requeridas por las autoridades. 4. Los sujetos mencionados en los apartados 1 y 2 de este artículo quedarán sujetos a la responsabilidad regulada en el apartado 3 del artículo 588 ter e. **Artículo 588 septies c. Duración:** La medida tendrá una duración máxima de un mes, prorrogable por iguales períodos hasta un máximo de tres meses.»
9	OSINT	**No se encontró medida especial aplicable.**
10	Acceso transfronterizo de datos	**Artículo 588 sexies c. Autorización judicial:** 1. La resolución del juez de instrucción mediante la que se autorice el acceso a la información contenida en los dispositivos a que se refiere la presente sección, fijará los términos y el alcance del registro y podrá autorizar la realización de copias de los datos informáticos. Fijará también las condiciones necesarias para asegurar la integridad de los datos y las garantías de su preservación para hacer posible, en su caso, la práctica de un dictamen pericial. 2. Salvo que constituyan el objeto o instrumento del delito o existan otras razones que lo justifiquen, se evitará la incautación de los soportes físicos que

Nº	Medidas de investigación	Regulación de medidas de investigación en España
		contengan los datos o archivos informáticos, cuando ello pueda causar un grave perjuicio a su titular o propietario y sea posible la obtención de una copia de ellos en condiciones que garanticen la autenticidad e integridad de los datos. 3. Cuando quienes lleven a cabo el registro o tengan acceso al sistema de información o a una parte del mismo conforme a lo dispuesto en este capítulo, tengan razones fundadas para considerar que los datos buscados están almacenados en otro sistema informático o en una parte de él, podrán ampliar el registro, siempre que los datos sean lícitamente accesibles por medio del sistema inicial o estén disponibles para este. Esta ampliación del registro deberá ser autorizada por el juez, salvo que ya lo hubiera sido en la autorización inicial. En caso de urgencia, la Policía Judicial o el fiscal podrán llevarlo a cabo, informando al juez inmediatamente, y en todo caso dentro del plazo máximo de veinticuatro horas, de la actuación realizada, la forma en que se ha efectuado y su resultado. El juez competente, también de forma motivada, revocará o confirmará tal actuación en un plazo máximo de setenta y dos horas desde que fue ordenada la interceptación. 4. En los casos de urgencia en que se aprecie un interés constitucional legítimo que haga imprescindible la medida prevista en los apartados anteriores de este artículo, la Policía Judicial podrá llevar a cabo el examen directo de los datos contenidos en el dispositivo incautado, comunicándolo inmediatamente, y en todo caso dentro del plazo máximo de veinticuatro horas, por escrito motivado al juez competente, haciendo constar las razones que justificaron la adopción de la medida, la actuación realizada, la forma en que se ha efectuado y su resultado. El juez competente, también de forma motivada, revocará o confirmará tal actuación en un plazo máximo de 72 horas desde que fue ordenada la medida. 5. Las autoridades y agentes encargados de la investigación podrán ordenar a cualquier persona que conozca el funcionamiento del sistema informático o las medidas aplicadas para proteger los datos informáticos contenidos en el mismo que facilite la información que resulte necesaria, siempre que de ello no derive una carga desproporcionada para el afectado, bajo apercibimiento de incurrir en delito de desobediencia. Esta disposición no será aplicable al investigado o encausado, a las personas que están dispensadas de la obligación de declarar por razón de parentesco y a aquellas que, de conformidad con el artículo 416.2, no pueden declarar en virtud del secreto profesional.»
11	Hallazgos casuales en evidencia digital	**- Parcialmente aplicable - Artículo 579 bis. Utilización de la información obtenida en un procedimiento distinto y descubrimientos casuales:** 1. El resultado de la detención y apertura de la correspondencia escrita y telegráfica podrá ser utilizado como medio de investigación o prueba en otro proceso penal. 2. A tal efecto, se procederá a la deducción de testimonio de los particulares necesarios para acreditar la legitimidad de la injerencia. Se incluirán entre los antecedentes indispensables, en todo caso, la solicitud inicial para la adopción, la resolución judicial que la acuerda y todas las peticiones y resoluciones judiciales de prórroga recaídas en el procedimiento de origen. 3. La continuación de esta medida para la investigación del delito casualmente descubierto requiere autorización del juez competente, para la cual, éste comprobará la diligencia de la actuación, evaluando el marco en el que se produjo el hallazgo casual y la imposibilidad de haber solicitado la medida que lo

Nº	Medidas de investigación	Regulación de medidas de investigación en España
		incluyera en su momento. Asimismo se informará si las diligencias continúan declaradas secretas, a los efectos de que tal declaración sea respetada en el otro proceso penal, comunicando el momento en el que dicho secreto se alce.»
12	Desbloqueo compulsivo de datos informáticos	**No se encontró medida especial aplicable.**

Tabla Nº 33: Resumen de medidas de investigación reguladas en España

7.6.3. Orden de conservación de datos

La última medida vinculada a las actuaciones de investigación introducidas por la LO 13/2015 es la orden de conservación de datos archivados, recogida en el Capítulo X del Título VIII del Libro II de la Ley de Enjuiciamiento Criminal, y conformado por el art. 588 octies. La medida consiste en el requerimiento a cualquier persona física o jurídica, por parte de la policía judicial o el ministerio fiscal, de la conservación y protección de datos incluidos en un sistema informático de almacenamiento (por ejemplo lo que venimos conociendo como “la nube”) hasta la obtención de la necesaria autorización judicial para su cesión.

En lo que respecta a la duración de la medida, tendrá una duración máxima inicial de noventa días, prorrogable hasta la autorización de la cesión de la información o el cumplimiento de ciento ochenta días.

El requerido vendrá obligado a prestar su colaboración y a guardar secreto del desarrollo de esta diligencia, quedando sujeto a la responsabilidad descrita en el apartado 3 del art. 588 ter e) pudiendo incurrir en un delito de desobediencia.

7.6.4. Acceso a datos necesarios para la identificación de usuarios y dispositivos

Dentro de esta novedosa medida de investigación, se distinguen tres supuestos diferentes según la identificación a la que se tenga acceso y que reproducimos seguidamente:

7.6.4.1. Identificación por dirección IP

El primer caso es para la identificación mediante número IP (art. 588 ter k) que establece la posibilidad de solicitar a través del juez de instrucción que requiera de los agentes sujetos al deber de colaboración según el art. 588 ter e, la cesión de los datos que permitan la identificación y localización del terminal o del dispositivo de conectividad y la identificación del sospechoso.

Es decir, esta herramienta regula algo muy utilizado en el marco de las investigaciones penales, que básicamente es la posibilidad de que al momento de tener la dirección IP de una conexión bajo investigación (que puede ser brindada incluso por la víctima del ciberdelito), se pueda gestionar un acceso a la información (tanto a la titularidad como a la ubicación geográfica) a través del pedido realizado por el juez.

En este caso, a diferencia de lo que sucede en otros países como Argentina, hacemos notar que el acceso a datos básicos de suscriptor (BSI) como podrían ser los datos identificatorios (nombre, apellido, domicilio de facturación, forma de pago, etc.) podrían ser solicitados directamente por la Fiscalía a cargo de la investigación, sin necesidad de requerir autorización judicial. A nuestro criterio, creemos que dicho requisito tiene más que ver con la posibilidad de acceder a la localización de la persona, dato que ya implica un mayor nivel de afectación de la intimidad.

De otra forma, entendemos que el mero acceso a los datos de abonado de un IP no debería requerir previa autorización judicial, en coherencia con lo regulado en

el propio artículo 588 ter m. explicado más adelante (relacionado a la identificación de titulares, terminales o dispositivos).

7.6.4.2. Identificación de terminales mediante captación de códigos de identificación

A través del art. 588 ter l España ha regulado la posibilidad de identificación de los terminales mediante captación de códigos de identificación del aparato o de sus componentes.

Para ello, la normativa establece un requisito preliminar: la imposibilidad de obtener un determinado número de abonado y este resulte indispensable a los fines de la investigación. Es decir, antes de avanzar en este tipo de técnicas, el legislador se ha querido asegurar que podría existir un camino más directo hacia la información de interés.

¿En qué casos podría ser imposible obtener el número de abonado? Por ejemplo, ante casos de conexión que utilicen tecnología de NATEO, ante casos de conexiones realizadas desde tarjetas de celular cuya titularidad no es real, ante casos de conexiones realizadas desde conexiones a internet públicas, entre otros tantos.

En estos casos, los agentes de Policía Judicial podrán valerse de artificios técnicos que permitan acceder al conocimiento de los códigos de identificación o etiquetas técnicas del aparato de telecomunicación o de alguno de sus componentes, tales como la numeración IMSI o IMEI y, en general, de cualquier medio técnico que, de acuerdo con el estado de la tecnología, sea apto para identificar el equipo de comunicación utilizado o la tarjeta utilizada para acceder a la red de telecomunicaciones.

Entre los artificios técnicos que podrían implementarse, podrían ser los ya desarrollados en el apartado de medidas especiales de investigación, referidas en particular en la sección 6.3.4. de este tesis, referida a la técnica de identificación de dispositivo por Browser fingerprinting.

7.6.4.3. Identificación de titulares, dispositivos o terminales

A través del art. 588 ter m. se introduce la tercera opción dentro de la sección de la Sección 3ra. dedicada al "Acceso a los datos necesarios para la identificación de usuarios, terminales y dispositivos de conectividad".

Este artículo establece la posibilidad de que cuando cuando el Ministerio Fiscal o la Policía Judicial necesiten conocer la titularidad de un número de teléfono o de cualquier otro medio de comunicación, o, en sentido inverso, precisen el número de teléfono o los datos identificativos de cualquier medio de comunicación, podrán dirigirse directamente a los prestadores de servicios de telecomunicaciones, quienes estarán obligados a cumplir el requerimiento, bajo apercibimiento de incurrir en el delito de desobediencia.

Es decir, básicamente regula la tan utilizada medida de pedir a un prestador de comunicaciones, la titularidad de una línea telefónica. Como explicamos anteriormente en el punto 7.6.4.1. aquí el artículo no establece la obligación de solicitar dicha información previa autorización judicial, sino que establece que la misma podrá ser solicitada directamente por el Ministerio Fiscal o la Policía Judicial, entendiendo que sólo se accederá a información de BSI, que cómo hemos visto en el capítulo V de la presente tesis, su afectación de la privacidad no ameritaría (en principio) la necesidad de una autorización judicial.

7.6.5. Registro de dispositivos de almacenamiento masivo de información

De acuerdo al art. 588 sexies a. será posible pedir, en el marco de un registro domiciliario, un registro de dispositivos de almacenamientos masivo de información, siempre que se justifique ante el juez que emite la orden, la necesidad o las razones que legitiman el acceso de los agentes a la información contenida en los dispositivos.

De forma muy clara e importante para los potenciales cuestionamientos que puedan darse desde la defensa penal, el inciso 2 establece que la simple incautación de cualquiera de los dispositivos a los que se refiere el apartado anterior, practicada durante el transcurso de la diligencia de registro domiciliario, no legitima el acceso a su contenido, sin perjuicio de que dicho acceso pueda ser autorizado ulteriormente por el juez competente.

Es decir, la autorización al secuestro de los dispositivos, no implica la autorización al acceso a la información. Si bien actualmente hay una tendencia a evitar llevarse tantos equipos informáticos (por razones antes explicadas, sobre todo en el tema de cifrado de datos), lo cierto es que avanzar sobre el acceso a los datos en el marco del registro domiciliario, siempre debe estar previamente autorizado por la autoridad judicial competente.

Para el caso de dispositivos electrónicos incautados fuera del domicilio del investigado, el art. 588 sexies b. se aplicarán las mismas reglas antes definidas, es decir, que en el caso que sea considerado indispensable el acceso a la información albergada en su contenido, deberá solicitarse la correspondiente autorización.

A modo de opciones, el art. 588 sexies c. establece que la autorización del juez fijará los términos y el alcance del registro y podrá autorizar la realización de copias de los datos informáticos, algo que nos parece adecuado. Sin embargo, sobre el final del precitado artículo, establece también que el juez fijará también *"las condiciones necesarias para asegurar la integridad de los datos y las garantías de su preservación para hacer posible, en su caso, la práctica de un dictamen pericial"*. En este punto ya no coincidimos tanto, toda vez que opinamos que serán las personas especializadas de realizar dichas recolecciones de dispositivos o de información, las que deberán estar adecuadamente capacitadas para, de acuerdo al caso concreto, al tipo de información, a la forma de recolección, etc, establecer y decidir en el momento, las prácticas o medidas más adecuadas que permitan garantizar la cadena de custodia de los elementos secuestrados. Pedir que un juez, desde la lejanía que puede tener de la práctica concreta de ese caso, y de lo que eventualmente se encuentren en dicho registro domiciliario, pueda fijar anticipadamente las condiciones necesarias para asegurar la integridad de los datos.

Por otro lado, en el inc. 2 del precitado artículo establece establece sanamente el criterio antes mencionado acerca de evitar en la medida de lo posible la incautación de los soportes físicos que contengan los datos, máximo cuando ello pueda causar un grave perjuicio a su titular o propietario y sea posible la obtención de una copia de ellos en condiciones que garanticen la autenticidad e integridad de los datos.

7.6.6. La extensión de registros

Continuando con el análisis del art. 588 sexies c. inc. 3, destacamos la existencia de un párrafo que hace referencia a los casos donde cuando en el acceso a datos en un sistema informático, "*existan razones fundadas para considerar que los datos buscados están almacenados en otro sistema informático o en una parte de él, podrán ampliar el registro, siempre que los datos sean lícitamente accesibles por medio del sistema inicial o estén disponibles para este*".

No queda claro si esto permitiría o sería parte de una regulación sobre el acceso transfronterizo de datos, toda vez que no hace referencia a datos que se encuentren fuera de la jurisdicción española, sin embargo, tampoco dice lo contrario. Quizás, hasta el concepto de datos que sean "lícitamente accesibles", es una forma de legitimar preliminarmente estos acceso, aunque a posteriori los mismos queden a control judicial.

A nuestro criterio, es una norma que perfectamente podemos considerar aplicable en la actualidad a casos de acceso transfronterizo de datos, por lo que hemos considerado como positivo su hallazgo.

En cualquiera de los casos esta ampliación del registro deberá ser autorizada por el juez, salvo que ya lo hubiera sido en la autorización inicial.

7.6.7. El acceso a los datos ante casos de urgencia

La Ley de Enjuiciamiento Criminal establece, sobre el final del art. 588 sexies c. que las ampliaciones en caso de urgencia, autoriza a que la Policía Judicial o el fiscal puedan llevar a cabo esta extensión de registros, informando al juez inmediatamente, y en todo caso dentro del plazo máximo de veinticuatro horas, de la actuación realizada, la forma en que se ha efectuado y su resultado. El juez competente, también de forma motivada, revocará o confirmará tal actuación en un plazo máximo de setenta y dos horas desde que fue ordenada la interceptación.

Adicionalmente, el inc. 4 establece que en los casos de urgencia en que se aprecie un interés constitucional legítimo que haga imprescindible la medida del acceso a los datos (aunque no existe una potencial extensión de registros), la norma autoriza también que la Policía Judicial podrá llevar a cabo el examen directo de los datos contenidos en el dispositivo incautado, comunicándolo inmediatamente, y en todo caso dentro del plazo máximo de veinticuatro horas, por escrito motivado al juez competente, haciendo constar las razones que justificaron la adopción de la medida, la actuación realizada, la forma en que se ha efectuado y su resultado. El juez competente, también de forma motivada, revocará o confirmará tal actuación en un plazo máximo de 72 horas desde que fue ordenada la medida.

7.6.8. La colaboración de personas que tengan conocimiento del sistema informático

El inc. 5 del artículo analizado, trae quizás uno de las medidas más cuestionadas a nivel internacional, como lo hemos visto anteriormente en el caso del Proyecto de ONU, al cuál hacemos referencia a la sección 4.3.2.

España ha legislado que "*las autoridades y agentes encargados de la investigación podrán ordenar a cualquier persona que conozca el funcionamiento del sistema informático o las medidas aplicadas para proteger los datos informáticos contenidos en el mismo que facilite la información que resulte necesaria, siempre*

que de ello no derive una carga desproporcionada para el afectado, bajo apercibimiento de incurrir en delito de desobediencia".

Adicionalmente se establece que dicha disposición no será aplicable al investigado o encausado, a las personas que están dispensadas de la obligación de declarar por razón de parentesco y a aquellas que, de conformidad con el artículo 416.2, no pueden declarar en virtud del secreto profesional.

Es decir, las personas que tengan conocimiento sobre el funcionamiento de los sistemas (por ejemplo un administrador de sistemas, un empleado con accesos, un profesional de la seguridad que tenga conocimientos especializados?) tendrá la obligación de proporcionar información sobre los sistemas que se administren, bajo pena de delito si no se obedece.

La clave para equilibrar esta regla, pareciera estar en el concepto que *"siempre que de ello no derive una carga desproporcionada para el afectado*". Sería interesante profundizar sobre esta obligación, ya que si bien está claro el objetivo del legislador, toda vez que si uno piensa la regla en el marco de un allanamiento en las instalaciones de una empresa, es clave la cooperación por parte de los encargados de sistemas.

Sin embargo, si se piensa la misma regla, bajo un registro domiciliario y la colaboración que se pide es a una persona totalmente ajena a la escena, como podría ser un hacker (profesional de la seguridad de la información) que por sus conocimientos, pueda vulnerar dicho sistema permitiendo el acceso a los datos, quizás parece un poco desproporcionado.

Cualquiera sea su interpretación, dejamos aquí otra posta para futuras continuaciones de esta investigación, o que otra persona podría tener interés en continuar desarrollando, a fin de profundizar con mayor nivel de rigurosidad esta norma y sus aplicaciones en la práctica de las investigaciones penales.

7.6.9. Incorporación al proceso de datos electrónicos de tráfico o asociados

En cuanto a los datos obrantes en archivos automatizados de los prestadores de servicios, el art. 588 ter j) establece que "*los datos electrónicos conservados por los prestadores de servicios o personas que faciliten la comunicación en cumplimiento de la legislación sobre retención de datos relativos a las comunicaciones electrónicas o por propia iniciativa por motivos comerciales o de otra índole y que se encuentren vinculados a procesos de comunicación, solo podrán ser cedidos para su incorporación al proceso con autorización judicial*".

Es decir, la normativa española avala que el acceso a los datos de tráfico, pueden realizarse sólo previa autorización judicial. De hecho, el segundo párrafo del citado artículo agrega información en cuanto a la necesidad de fundamentos del pedido, toda vez que podrán ser solicitados "*cuando el conocimiento de esos datos resulte indispensable para la investigación*".

7.6.10. La posibilidad de registro remoto

El artículo 588 septies a. establece que el juez competente podrá autorizar la utilización de datos de identificación y códigos, así como la instalación de un software, que permitan, de forma remota y telemática, el examen a distancia y sin conocimiento de su titular o usuario del contenido de un ordenador, dispositivo electrónico, sistema informático, instrumento de almacenamiento masivo de datos informáticos o base de datos.

Esta herramienta investigativa, considerando su gran potencial de afectación a derechos y garantías, ha sido limitada para la investigación de determinadas categorías de delitos que, a prima facie, son de gravedad, tales como: a) Delitos cometidos en el seno de organizaciones criminales. b) Delitos de terrorismo. c) Delitos cometidos contra menores o personas con capacidad modificada judicialmente. d) Delitos contra la Constitución, de traición y relativos a la defensa

nacional. e) Delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la telecomunicación o servicio de comunicación.

Es quizás el último inciso e, la categoría que más dudas puede dejar frente a su gravedad, toda vez que el hecho que sea cometido a través de instrumentos informáticos no presume de por sí, la gravedad del hecho cometido.

En relación a los límites regulados, la resolución judicial que autorice el registro deberá especificar los equipos o sistemas objeto de la medida, la forma en la que se procederá al acceso a los datos, el software que será utilizado y los agentes autorizados. Luego se hace referencia a la autorización de realización de copia de la información y su preservación, aspectos que en este nivel de medidas de investigación, son básicos.

Nos parece de interés hacer algunas breves referencias al respecto de estos requisitos, que tal como hemos señalado sobre la norma regulada para la Provincia de Salta (Argentina), dependiendo del tipo de caso, es muy probable que pueda no tenerse al momento del dictado de la resolución judicial demasiada certeza técnica que permita dar tantas precisiones.

Está clara la intención del legislador en este sentido, que cuanta más precisiones tenga la orden judicial, más posibilidades tendremos de llevar adelante un control exitoso de la medida.

Igual comentario podemos realizar en cuanto a la precisión acerca de la “forma” de acceso, toda vez que dependerá exclusivamente de la tecnología disponible, el sistema al cuál se pretende ingresar, etc.

Cabe la posibilidad de autorizar una ampliación del registro cuando existan razones para creer que los datos requeridos se encuentran en otro dispositivo informático. De forma análoga al resto de medidas, se fija un deber de colaboración según el cual las autoridades pueden ordenar la facilitación de información necesaria para el buen fin de la diligencia, a aquellas personas que conozcan el funcionamiento del concreto sistema informático.

En este sentido el art. 588 septies b) establece este deber de colaboración en relación especialmente con las siguientes personas: los prestadores de servicios y

personas señaladas en el art. 588 ter e) los titulares o responsables del sistema informático o base de datos objeto del registro y cualquier persona que conozca el funcionamiento del sistema informático o las medidas aplicadas para proteger los datos informáticos contenidos en el mismo. Los sujetos requeridos para prestar colaboración tendrán la obligación de guardar secreto acerca de las actividades requeridas por las autoridades.

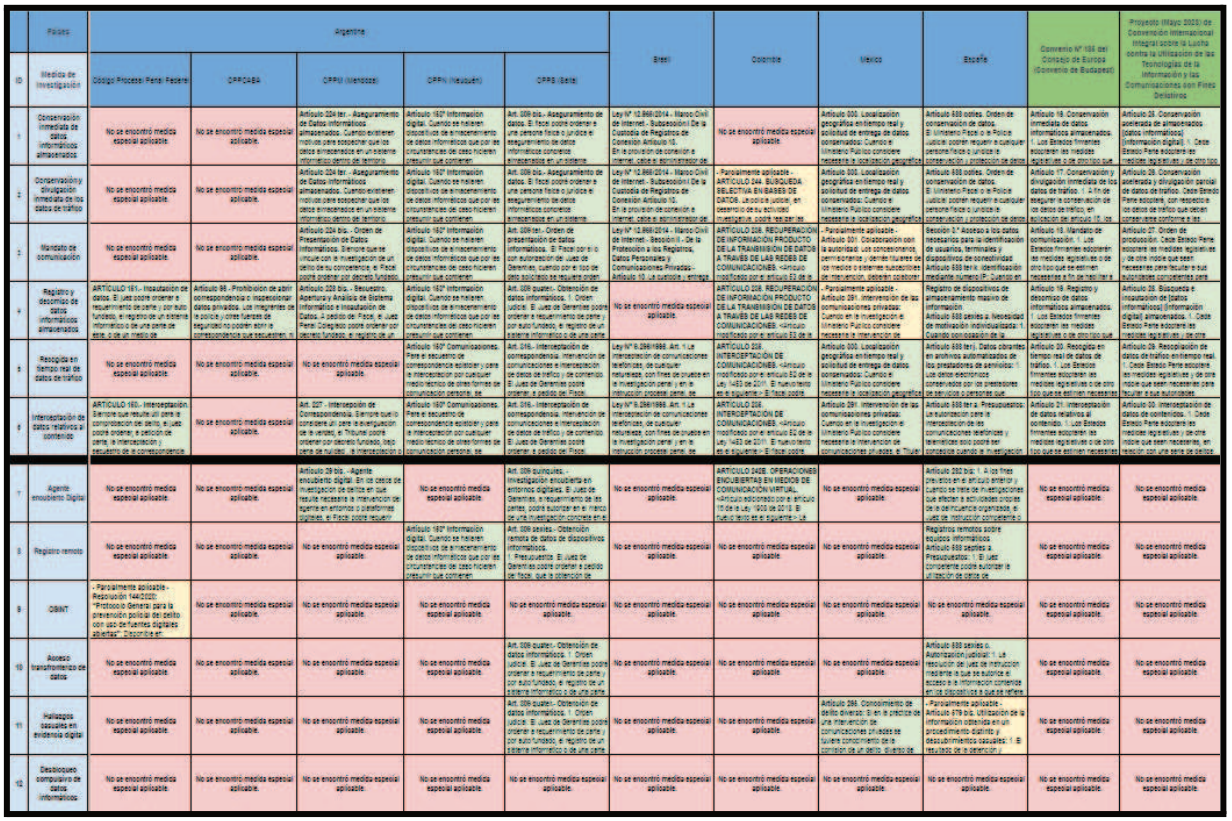
Por último, en lo que respecta al tiempo de duración, la medida no ha de durar más del tiempo estrictamente necesario para el esclarecimiento de los hechos objeto de investigación. Concretamente se prevé que la duración máxima sea de un mes, prorrogable por iguales períodos hasta un máximo de tres meses.

7.7. Generación de estadísticas

A partir de aquí, resumimos los resultados alcanzados con la construcción de estadísticas calculadas a partir de los resultados obtenidos en el estudio de derecho comparado del aspecto procesal penal.

Recordamos que en los casos donde consideramos que la medida de investigación penal estudiada no se encuentra tipificada en su totalidad, pero existen medidas de investigación similares o que podrían ser aplicables a los mismos fines, se ha optado por señalarlos en las tablas como “parcialmente aplicables”.

Si bien por cuestiones de espacio y por la cantidad de texto de los artículos relevados, es imposible reproducir la siguiente tabla de forma que sea visualmente claro para la persona lectora, reproducimos una imagen en miniatura de la planilla comparativa realizada con todo el relevamiento en materia procesal penal.



ID	Países	Argentina					Brasil	Colombia	México	España	Convenio N° 185 del Consejo de Europa (Convenio de Budapest)	Proyecto (Mayo 2023) de Convención internacional integral sobre la Lucha contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos
	Medida de investigación	Código Procesal Penal Federal	CPPCABA	CPPM (Mendoza)	CPPN (Neuquén)	CPPS (Salta)						
1	Conservación inmediata de datos informáticos almacenados	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	Artículo 224 ter.- Aseguramiento de Datos Informáticos almacenados. Cuando existieren motivos para sospechar que los datos almacenados en un sistema informático dentro de territorio	Artículo 187° Información digital. Cuando se hallaren dispositivos de almacenamiento de datos informáticos que por las circunstancias del caso hicieren presumir que contienen	Art. 228 bis.- Aseguramiento de datos. El Fiscal podrá ordenar a una persona física o jurídica el aseguramiento de datos informáticos concretos almacenados en un sistema	Ley N° 12.965/2014 - Marco Civil de Internet - Subsección I De la Custodia de Registros de Conexión Artículo 10. En la provisión de conexión a internet, cabe a administrador de	No se encontró medida especial aplicable.	Artículo 000. Localización geográfica en tiempo real y solicitud de entrega de datos conservados: Cuerpo e Ministerio Público considere necesaria la colocación geográfica	Artículo 588 octies. Orden de conservación de datos. El Ministerio Fiscal o la Policía Judicial podrán requerir a cualquier persona física o jurídica la conservación y protección de datos	Artículo 16. Conservación inmediata de datos informáticos almacenados. 1. Los Estados firmantes adoptarán las medidas que sean	Artículo 28. Conservación acelerada de almacenados datos informáticos almacenados. [Información digital] 1. Cada Estado Parte adoptará las medidas que sean
2	Conservación y divulgación inmediata de los datos de tráfico	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	Artículo 224 ter.- Aseguramiento de Datos Informáticos almacenados. Cuando existieren motivos para sospechar que los datos almacenados en un sistema informático dentro de territorio	Artículo 187° Información digital. Cuando se hallaren dispositivos de almacenamiento de datos informáticos que por las circunstancias del caso hicieren presumir que contienen	Art. 228 bis.- Aseguramiento de datos. El Fiscal podrá ordenar a una persona física o jurídica el aseguramiento de datos informáticos concretos almacenados en un sistema	Ley N° 12.965/2014 - Marco Civil de Internet - Subsección I De la Custodia de Registros de Conexión Artículo 10. En la provisión de conexión a internet, cabe a administrador de	- Paralelamente aplicable - ARTÍCULO 244. BÚSQUEDA SELECTIVA EN BANASES DE DATOS. La policía judicial, en desarrollo de su actividad investigativa podrá, de oficio	Artículo 000. Localización geográfica en tiempo real y solicitud de entrega de datos conservados: Cuerpo e Ministerio Público considere necesaria la colocación geográfica	Artículo 588 octies. Orden de conservación de datos. El Ministerio Fiscal o la Policía Judicial podrán requerir a cualquier persona física o jurídica la conservación y protección de datos	Artículo 17. Conservación y divulgación inmediata de los datos de tráfico. 1. A fin de asegurar la conservación de los datos de tráfico, en aplicación del artículo 16, los	Artículo 29. Conservación preservada y divulgación parcial de datos de tráfico. Cada Estado Parte adoptará, con respecto a los datos de tráfico que serán conservados conforme a lo
3	Mandato de comunicación	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	Artículo 224 bis.- Orden de Presentación de Datos Informáticos. Siempre que se vincule con la investigación de un delito de su competencia, el Fiscal podrá ordenar por decreto fundado	Artículo 187° Información digital. Cuando se hallaren dispositivos de almacenamiento de datos informáticos que por las circunstancias del caso hicieren presumir que contienen	Art. 228 ter.- Orden de presentación de datos informáticos. El Fiscal podrá ordenar a una persona física o jurídica el cumplimiento de una orden de Decreto, cuando por el tipo de otro solicitado se requiera orden	Ley N° 12.965/2014 - Marco Civil de Internet - Sección II - De la Protección a los Registros, Datos Personales y Comunicaciones Privadas - Artículo 10. Los custodios y entrega	ARTÍCULO 238. RECUPERACIÓN DE INFORMACIÓN PRODUCTO DE LA TRANSMISIÓN DE DATOS A TRAVÉS DE LAS REDES DE COMUNICACIONES. <Artículo modificado por el artículo 53 de la	- Paralelamente aplicable - Artículo 591. Colaboración con la autoridad. Los concesionarios, permisionarios y demás titulares de los medios o sistemas susceptibles de transmisión, deberán cooperar	Sección 3.ª Acceso a los datos necesarios para la identificación de usuarios, terminales y dispositivos de conectividad Artículo 588 ter k. Identificación mediante número IP. Cuando en	Artículo 18. Mandato de comunicación. 1. Los Estados firmantes adoptarán las medidas legislativas que sean necesarias para facultar a sus autoridades competentes para	Artículo 27. Orden de producción. Cada Estado Parte adoptará las medidas legislativas que sean necesarias para facultar a sus autoridades competentes para
4	Registro y desarrollo de datos informáticos almacenados	ARTÍCULO 161.- Inhabilitación de datos. El juez podrá ordenar a requerimiento de parte y por auto fundado, el registro de un sistema informático o de una parte de éste, o de un medio de	Artículo 96.-Prohibición de abrir correspondencia e inspeccionar datos privados. Los integrantes de la policía y otros fuerzas de seguridad no podrán abrir la correspondencia que secuestren,	Artículo 229 bis.- Secuestro. Apertura y Análisis de Sistema Informático e Incautación de Datos. A pedido de Fiscal, el Juez Penal Colegiado podrá ordenar por decreto fundado, el registro de un	Artículo 187° Información digital. Cuando se hallaren dispositivos de almacenamiento de datos informáticos que por las circunstancias del caso hicieren presumir que contienen	Art. 228 quater.- Obtención de datos informáticos. 1. Orden judicial. El juez de Garantías podrá ordenar a requerimiento de parte y por auto fundado, el registro de un sistema informático o de una parte	No se encontró medida especial aplicable.	ARTÍCULO 238. RECUPERACIÓN DE INFORMACIÓN PRODUCTO DE LA TRANSMISIÓN DE DATOS A TRAVÉS DE LAS REDES DE COMUNICACIONES. <Artículo modificado por el artículo 53 de la	- Paralelamente aplicable - Artículo 591. Intervención de las comunicaciones privadas: Cuando en la investigación el Ministerio Público considere necesaria la intervención de	Sección 3.ª Acceso a los datos necesarios para la identificación de usuarios, terminales y dispositivos de conectividad Artículo 588 ter k. Identificación mediante número IP. Cuando en	Artículo 19. Registro y desarrollo de datos informáticos almacenados. 1. Los Estados firmantes adoptarán las medidas legislativas que sean necesarias para facultar a sus autoridades competentes para	Artículo 28. Búsqueda e incautación de [datos informáticos] [información digital] almacenados. 1. Cada Estado Parte adoptará las medidas que sean necesarias para facultar a sus autoridades competentes para
5	Recogida en tiempo real de datos de tráfico	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	Artículo 187° Comunicaciones. Para el secuestro de correspondencia epistolar y para la intervención por cualquier medio técnico de otras formas de comunicación personal, se	Art. 236.- Intercepción de correspondencia. Intervención de comunicaciones e intercepción de datos de tráfico y de contenido. El Juez de Garantías podrá ordenar, a pedido del Fiscal,	Ley N° 9.296/1996. Art. 1.La intercepción de comunicaciones telefónicas, de cualquier naturaleza, con fines de prueba en la investigación penal y en la instrucción procesal penal, de	ARTÍCULO 238. INTERCEPTACIÓN DE COMUNICACIONES. <Artículo modificado por el artículo 52 de la Ley 1453 de 2011> El fiscal podrá en el siguiente: El fiscal podrá	Artículo 000. Localización geográfica en tiempo real y solicitud de entrega de datos conservados: Cuerpo e Ministerio Público considere necesaria la colocación geográfica	Artículo 588 terj. Datos obrantes en archivos automatizados de los prestadores de servicios: 1. Los datos electrónicos conservados por los prestadores de servicios o personas que	Artículo 20. Recogida en tiempo real de datos de tráfico. 1. Los Estados firmantes adoptarán las medidas legislativas y de otro tipo que se estimen necesarias	Artículo 29. Recopilación de datos de tráfico en tiempo real. 1. Cada Estado Parte adoptará las medidas legislativas y de otra índole que sean necesarias para
6	Intercepción de datos relativos al contenido	ARTÍCULO 193.- Intercepción. Siempre que resulte útil para la comprobación del delito, el juez podrá ordenar, a petición de parte, la intercepción y secuestro de la correspondencia		Art. 227 - Intercepción de Correspondencia. Siempre que lo considere útil para la averiguación de la verdad, el Tribunal podrá ordenar por decreto fundado, bajo pena de nulidad, la intercepción o	Artículo 187° Comunicaciones. Para el secuestro de correspondencia epistolar y para la intercepción por cualquier medio técnico de otras formas de comunicación personal, se	Art. 236.- Intercepción de correspondencia. Intervención de comunicaciones e intercepción de datos de tráfico y de contenido. El Juez de Garantías podrá ordenar, a pedido del Fiscal,	Ley N° 9.296/1996. Art. 1.La intercepción de comunicaciones telefónicas, de cualquier naturaleza, con fines de prueba en la investigación penal y en la instrucción procesal penal, de	ARTÍCULO 238. INTERCEPTACIÓN DE COMUNICACIONES. <Artículo modificado por el artículo 52 de la Ley 1453 de 2011> El fiscal podrá en el siguiente: El fiscal podrá	Artículo 000. Localización geográfica en tiempo real y solicitud de entrega de datos conservados: Cuerpo e Ministerio Público considere necesaria la colocación geográfica	Artículo 588 terj. Presupuestos. La autorización para la intercepción de las comunicaciones telefónicas y telemáticas sólo podrá ser concedida cuando la investigación	Artículo 21. Intercepción de datos relativos al contenido. 1. Los Estados firmantes adoptarán las medidas legislativas y de otro tipo que se estimen necesarias	Artículo 30. Intercepción de datos de contenidos. 1. Cada Estado Parte adoptará las medidas legislativas y de otra índole que sean necesarias, en relación con una serie de delitos
7	Agente encubierto Digital	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	Artículo 29 bis. - Agente encubierto digital. En los casos de investigación de delitos en que resulte necesaria la intervención de agentes en entornos o plataformas digitales, el Fiscal podrá requerir	No se encontró medida especial aplicable.	Art. 228 quinquies. - Investigación encubierta en entornos digitales. El Juez de Garantías, a requerimiento de las partes, podrá autorizar en el marco de una investigación concreta en la	No se encontró medida especial aplicable.	ARTÍCULO 242B. OPERACIONES ENCUBIERTAS EN MEDIOS DE COMUNICACIÓN VIRTUAL. <Artículo adicionado por el artículo 15 de la Ley 1908 de 2018> El fiscal podrá en el siguiente: La	No se encontró medida especial aplicable.	Artículo 282 bis: 1. A los fines previstos en el artículo anterior y cuando se trate de investigaciones que afecten a actividades propias de la delincuencia organizada, el Juez de instrucción competente o	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.
8	Registro remoto	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	Artículo 187° Información digital. Cuando se hallaren dispositivos de almacenamiento de datos informáticos que por las circunstancias del caso hicieren presumir que contienen	Art. 228 sexies. - Obtención remota de datos de dispositivos informáticos. 1. Presupuesto. El Juez de Garantías podrá ordenar a pedido del Fiscal, que la obtención de	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	Registros remotos sobre equipos informáticos Artículo 588 septies a. Presupuestos. 1. El juez competente podrá autorizar la utilización de datos de	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.
9	OSINT	- Paralelamente aplicable - Resolución 144/2020: "Protocolo General para la prevención policial del delito con uso de fuentes digitales abiertas". Disponible en:	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.
10	Acceso transfronterizo de datos	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	Art. 228 quater.- Obtención de datos informáticos. 1. Orden judicial. El juez de Garantías podrá ordenar a requerimiento de parte y por auto fundado, el registro de un sistema informático o de una parte	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	Artículo 588 octies o. Autorización judicial: 1. La resolución del juez de instrucción mediante la que se autorice el acceso a la información contenida en los dispositivos a que se refiere	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.
11	Hallazgos casuales en evidencia digital	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	Art. 228 quater.- Obtención de datos informáticos. 1. Orden judicial. El juez de Garantías podrá ordenar a requerimiento de parte y por auto fundado, el registro de un sistema informático o de una parte	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	Artículo 286. Conocimiento de delito diverso. Si en la práctica de una intervención de comunicaciones privadas se tuviere conocimiento de la comisión de un delito distinto de	- Paralelamente aplicable - Artículo 579 bis. Utilización de la información obtenida en un procedimiento distinto y descubrimientos casuales: 1. El resultado de la aplicación	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.
12	Desbloqueo compulsivo de datos informáticos	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.

Tabla Nº 34: Cuadro general comparativo del estudio de derecho comparado sobre medidas de investigación reguladas en los países alcanzados por el estudio

A fin de poder exhibirlos de una forma más visible para la persona lectora, procederemos a la reproducción por partes de dicho cuadro, para posteriormente proceder a generar sus correspondientes estadísticas que nos brindarán el insumo necesario para avanzar hacia las conclusiones del estudio.

	Países	Argentina				
ID	Medida de Investigación	Código Procesal Penal Federal	CPPCABA	CPPM (Mendoza)	CPPN (Neuquén)	CPPS (Salta)

1	Conservación inmediata de datos informáticos almacenados	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	Artículo 224 ter.	Artículo 153	Art. 309 bis
2	Conservación y divulgación inmediata de los datos de tráfico	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	Artículo 224 ter.	Artículo 153	Art. 309 bis
3	Mandato de comunicación	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	Artículo 224 bis.	Artículo 153	Art. 309 ter
4	Registro y decomiso de datos informáticos almacenados	Artículo 151	Artículo 96 Artículo 119 Artículo 346	Artículo 228 bis	Artículo 153	Art. 309 quater
5	Recogida en tiempo real de datos de tráfico	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	Artículo 150	Art. 316
6	Interceptación de datos relativos al contenido	Artículo 150	No se encontró medida especial aplicable.	Art. 227 Art. 229 Art. 229 bis Art. 229 ter	Artículo 150	Art. 316
7	Agente encubierto Digital	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	Artículo 29 bis	No se encontró medida especial aplicable.	Art. 309 quinquies
8	Registro remoto	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	Artículo 153	Art. 309 sexies

9	OSINT	- Parcialmente aplicable - Resolución 144/2020	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.
10	Acceso transfronterizo de datos	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	Art. 309 quater
11	Hallazgos casuales en evidencia digital	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	Art. 309 quater
12	Desbloqueo compulsivo de datos informáticos	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.

Tabla Nº 35: Cuadro resumen de las medidas de investigación reguladas en Argentina

	Países	Brasil	Colombia	México	España
ID	Medida de Investigación				
1	Conservación inmediata de datos informáticos almacenados	Ley Nº 12.965/2014 Artículo 13 Artículo 15	No se encontró medida especial aplicable.	Artículo 303	Artículo 588 octies
2	Conservación y divulgación inmediata de los datos de tráfico	Ley Nº 12.965/2014 Artículo 13 Artículo 15	- Parcialmente aplicable - Artículo 244	Artículo 303	Artículo 588 octies
3	Mandato de comunicación	Ley Nº 12.965/2014 Artículo 10 Artículo 22 Artículo 23	Artículo 236	- Parcialmente aplicable - Artículo 301 Artículo 276	Artículo 588 ter k Artículo 588 ter l Artículo 588 ter m

4	Registro y decomiso de datos informáticos almacenados	No se encontró medida especial aplicable.	Artículo 236	- Parcialmente aplicable - Artículo 291 Artículo 292 Artículo 294	Artículo 588 sexies a Artículo 588 sexies b Artículo 588 sexies c
5	Recogida en tiempo real de datos de tráfico	Ley N° 9.296/1996. Art. 1	Artículo 235	Artículo 303	Artículo 588 ter j
6	Interceptación de datos relativos al contenido	Ley N° 9.296/1996. Art. 1	Artículo 235	Artículo 291 Artículo 292 Artículo 294	Artículo 588 ter a Artículo 588 ter b Artículo 588 ter c Artículo 588 ter d Artículo 588 ter e Artículo 588 ter f Artículo 588 ter g Artículo 588 ter h Artículo 588 ter i Artículo 588 quater a
7	Agente encubierto Digital	No se encontró medida especial aplicable.	Artículo 242B	No se encontró medida especial aplicable.	Artículo 282 bis
8	Registro remoto	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	Artículo 588 septies a Artículo 588 septies b Artículo 588 septies c
9	OSINT	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.
10	Acceso transfronterizo de datos	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	Artículo 588 sexies c

11	Hallazgos casuales en evidencia digital	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	Artículo 295	- Parcialmente aplicable - Artículo 579 bis
12	Desbloqueo compulsivo de datos informáticos	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.

Tabla Nº 36: Cuadro resumen de las medidas de investigación reguladas en Brasil, Colombia, México y España.

7.7.1. Regulación de medidas de investigación por países

El primero de los datos que es posible obtener, es sobre el nivel de regulación de las medidas de investigación por cada uno de los países. Por ello, se ha procedido a realizar un análisis cuantitativo sobre la cantidad de medidas o técnicas especiales de investigación cada país tiene reguladas, los cuáles en primera instancia son publicados con el orden de los países en los cuáles el estudio ha sido abordado.

Adicionalmente, separamos en un primer cuadro (a), la segmentación de medidas de 1 a 6, que son aquellas sugeridas por los instrumentos internacionales (y de interés para nuestra hipótesis de trabajo) y luego, en un segundo cuadro (b) más completo, la totalidad (12) de las medidas investigadas.

País		Medidas reguladas	Medidas parcialmente reguladas	Medidas no reguladas	Total
Argentina	Federal	33,33%	0,00%	66,67%	100,00%
	CABA	16,67%	0,00%	83,33%	100,00%
	Mendoza	83,33%	0,00%	16,67%	100,00%
	Neuquén	100,00%	0,00%	0,00%	100,00%

	Salta	100,00%	0,00%	0,00%	100,00%
Brasil		83,33%	0,00%	16,67%	100,00%
Colombia		66,67%	16,67%	16,67%	100,00%
México		66,67%	33,33%	0,00%	100,00%
España		100,00%	0,00%	0,00%	100,00%

Tabla Nº 37a: Cuadro comparativo de estadísticas de regulación de las medidas sugeridas internacional (1 a 6) (ordenados alfabéticamente)

País		Medidas reguladas	Medidas parcialmente reguladas	Medidas no reguladas	Total
Argentina	Federal	16,67%	8,33%	75,00%	100,00%
	CABA	8,33%	0,00%	91,67%	100,00%
	Mendoza	50,00%	0,00%	50,00%	100,00%
	Neuquén	58,33%	0,00%	41,67%	100,00%
	Salta	83,33%	0,00%	16,67%	100,00%
Brasil		41,67%	0,00%	58,33%	100,00%
Colombia		41,67%	8,33%	50,00%	100,00%
México		41,67%	16,67%	41,67%	100,00%
España		75,00%	8,33%	16,67%	100,00%

Tabla Nº 37b: Cuadro comparativo de estadísticas de regulación de la totalidad de las medidas de investigación para Delitos Informáticos (ordenados alfabéticamente)

En un segundo cuadro, estos mismos resultados han sido ordenados numéricamente generando una especie de "*ranking*" de los países (y provincias) que mayor regulación en materia procesal penal poseen al respecto.

Nuevamente, separamos en un primer cuadro (a), la segmentación de medidas de 1 a 6, que son aquellas sugeridas por los instrumentos internacionales (y de interés para nuestra hipótesis de trabajo) y luego, en un segundo cuadro (b) más completo, la totalidad (12) de las medidas investigadas.

Ranking	País	Medidas reguladas	Medidas parcialmente reguladas	Medidas no reguladas	Total
1	España	100,00%	0,00%	0,00%	100,00%
2	Argentina (Salta)	100,00%	0,00%	0,00%	100,00%
3	Argentina (Neuquén)	100,00%	0,00%	0,00%	100,00%
4	Argentina (Mendoza)	83,33%	0,00%	16,67%	100,00%
5	Brasil	83,33%	0,00%	16,67%	100,00%
6	Mexico	66,67%	33,33%	0,00%	100,00%
7	Colombia	66,67%	16,67%	16,67%	100,00%
8	Argentina (Federal)	33,33%	0,00%	66,67%	100,00%
9	Argentina (CABA)	16,67%	0,00%	83,33%	100,00%

Tabla Nº 38a: Ranking de estadísticas de regulación de medidas de investigación para Delitos Informáticos (ordenados por países y provincias con mayor nivel de cumplimiento)

Ranking	País	Medidas reguladas	Medidas parcialmente reguladas	Medidas no reguladas	Total
1	Argentina (Salta)	83,33%	0,00%	16,67%	100,00%
2	España	75,00%	8,33%	16,67%	100,00%
3	Argentina (Neuquén)	58,33%	0,00%	41,67%	100,00%
4	Argentina (Mendoza)	50,00%	0,00%	50,00%	100,00%
5	México	41,67%	16,67%	41,67%	100,00%
6	Colombia	41,67%	8,33%	50,00%	100,00%
7	Brasil	41,67%	0,00%	58,33%	100,00%

8	Argentina (Federal)	16,67%	8,33%	75,00%	100,00%
9	Argentina (CABA)	8,33%	0,00%	91,67%	100,00%

Tabla Nº 38b: Ranking de estadísticas de regulación de medidas de investigación para Delitos Informáticos (ordenados por países y provincias con mayor nivel de cumplimiento)

7.7.2. Nivel de regulación por medida de investigación

Como segundo dato de importancia que es posible obtener a partir de este estudio, consiste en analizar el nivel de regulación penal en todos los países alcanzados, de acuerdo a cada una de las medidas de investigación estudiadas.

De esta forma, podremos observar cuales son las medidas de investigación con mayor recepción y cuáles son aquellos que menor consenso tiene a nivel jurídico en el ámbito procesal penal de los países alcanzados.

Id	Medida de investigación	Reguladas	Parcialmente reguladas	No reguladas	Total
1	Conservación inmediata de datos informáticos almacenados	66,67%	0,00%	33,33%	100,00%
2	Conservación y divulgación inmediata de los datos de tráfico	66,67%	11,11%	22,22%	100,00%
3	Mandato de comunicación	66,67%	11,11%	22,22%	100,00%
4	Registro y decomiso de datos informáticos almacenados	77,78%	11,11%	11,11%	100,00%
5	Recogida en tiempo real de datos de tráfico	66,67%	0,00%	33,33%	100,00%
6	Interceptación de datos relativos al contenido	88,89%	0,00%	11,11%	100,00%
7	Agente encubierto Digital	44,44%	0,00%	55,56%	100,00%
8	Registro remoto	33,33%	0,00%	66,67%	100,00%
9	OSINT	0,00%	11,11%	88,89%	100,00%
10	Acceso transfronterizo de datos	22,22%	0,00%	77,78%	100,00%

11	Hallazgos casuales en evidencia digital	22,22%	11,11%	66,67%	100,00%
12	Desbloqueo compulsivo de datos informáticos	0,00%	0,00%	100,00%	100,00%

Tabla Nº 39: Estadísticas que indican en porcentajes el nivel de regulación de cada medida de investigación en la totalidad de los países incluídos en el estudio (ordenados de acuerdo al orden del análisis)

Ranking	Medida de investigación	Reguladas	Parcialmente reguladas	No reguladas	Total
1	Interceptación de datos relativos al contenido	88,89%	0,00%	11,11%	100,00%
2	Registro y decomiso de datos informáticos almacenados	77,78%	11,11%	11,11%	100,00%
3	Mandato de comunicación	66,67%	11,11%	22,22%	100,00%
4	Conservación y divulgación inmediata de los datos de tráfico	66,67%	11,11%	22,22%	100,00%
5	Recogida en tiempo real de datos de tráfico	66,67%	0,00%	33,33%	100,00%
6	Conservación inmediata de datos informáticos almacenados	66,67%	0,00%	33,33%	100,00%
7	Agente encubierto Digital	44,44%	0,00%	55,56%	100,00%
8	Registro remoto	33,33%	0,00%	66,67%	100,00%
9	Hallazgos casuales en evidencia digital	22,22%	11,11%	66,67%	100,00%
10	Acceso transfronterizo de datos	22,22%	0,00%	77,78%	100,00%
11	OSINT	0,00%	11,11%	88,89%	100,00%
12	Desbloqueo compulsivo de datos informáticos	0,00%	0,00%	100,00%	100,00%

Tabla Nº 40: Estadísticas que indican en porcentajes el nivel de regulación de cada medida de investigación en la totalidad de los países incluídos en el estudio (ordenados de acuerdo al nivel de regulación)

7.8. Análisis final sobre los resultados obtenidos

Comenzando por el caso de Argentina, si bien los resultados exhibidos no parecen ser para nada desalentadores, la persona lectora debe recordar que en nuestro país hemos abordado un estudio segmentado al momento de realizar la búsqueda de normativa que regule medidas de investigación relacionadas a la evidencia digital. Como hemos advertido dentro del estudio, hemos determinado como alcance al ámbito federal primero, y luego a Ciudad Autónomas de Buenos Aires, Mendoza, Neuquén y Salta, es decir que técnicamente hemos auditado aproximadamente un 20% de las jurisdicciones existentes.

Dejamos nota que hemos excluido de la revisión a las veinte Provincias restantes por considerar a prima facie que tenían un nulo o casi nulo desarrollo en la materia de interés. Por esto, es importante dimensionar los resultados alcanzados bajo ese contexto. A modo de ejemplo, es muy probable que el resto de las provincias no relevadas (20 en total), muchas dieran resultados similares a los encontrados en el fuero federal o en CABA, es decir, niveles de regulación menores al 20%.

Por eso, si bien nos alegramos de la existencia de la existencia de casos como Mendoza, Neuquén y sobre todo, de Salta, con niveles de regulación que oscilaron entre un 50 y un 83,33%, lo cierto es que estos resultados, a nivel país en Argentina, son más bien la excepción y no la regla.

Por otro lado, Argentina también tiene sus representantes ocupando los últimos dos lugares del ranking de la Tabla Nº 38, donde encontramos a CABA en el último lugar con un 8,33% de cumplimiento y en penúltimo lugar al ámbito federal, con apenas un 16,66%. Casi como un reflejo de muchos aspectos políticos, económicos y sociales, Argentina exhibe casos claros de éxito a nivel internacional, y aún así exhibe resultados de muy bajo rendimiento dejando en evidencia que aún tenemos una gran deuda en materia procesal penal, tanto en las provincias como a nivel federal.

Realizada esta aclaración, y enfocando estas conclusiones en los resultados estadísticos del estudio realizado, podemos citar que de acuerdo a la Tabla Nº 38, la Provincia de Salta ha logrado tener el 1er. lugar en el ranking (con un 83,33%) como jurisdicción que posee el nivel de regulación más alto (y por lo tanto, más completo) de todas las analizadas en el estudio, superando incluso a nuestra referencia europea, España. Es importante también destacar el aspecto cronológico, haciendo notar que la actualización salteña es mucho más reciente (2023) que la realizada a nivel país en España (2015).

Entre las novedades más importantes a destacar, claramente se encuentra el caso de la Provincia de Salta, que no sólo ha superado con creces la regulación de las medidas básicas sugeridas por el Convenio de Budapest, sino que ha optado por avanzar en la incorporación de varias de las medidas más modernas, donde podemos encontrar desde la figura de agente encubierto digital, el registro remoto, hasta una regulación incipiente sobre accesos transfronterizos de datos y hallazgos casuales en evidencia digital. Destacamos sobre todo la valentía de regular el acceso transfronterizo de datos, animándose a incorporar incluso un caso de habilitación extra a los ya validados en el art. 32 del Convenio de Cibercrimen de Budapest.

A su vez, Neuquén ha quedado en tercer lugar con un 58,33% de nivel de regulación, mientras que Mendoza, ha quedado en un cuarto lugar con un 41,67% (y un 16,67% de medidas parcialmente reguladas), destacando el gran nivel de regulación de estas provincias argentinas que han hecho punto en la materia de regular las medidas de investigación.

De Mendoza, es destacable que al momento de estar llevándose a cabo el estudio en sí mismo (finales 2023), se terminó de aprobar la figura del Agente Encubierto Digital, considerando a la misma como una flamante incorporación (que de hecho, en el primer análisis no se había tenido en cuenta porque no había completamente aprobada y promulgada).

En el caso de Neuquén, destacamos que ha sido la primera jurisdicción argentina que avanzó sobre la regulación en esta materia, teniendo también el valor de incorporar la posibilidad del registro remoto por primera vez en el país.

En relación al caso de Brasil, nos consideramos sorprendidos por el bajo nivel de regulación en materia procesal penal, toda vez que es un país que a nivel latinoamericano, siempre ha tenido buenos estándares en materia normativa, que por citar un ejemplo, sucede actualmente en materia de protección de datos, donde ellos han sido los primeros en regular siguiendo el modelo del Reglamento Europeo de Protección de Datos (GDPR).

Otro aspecto de interés a señalar, es que la mayoría de las medidas encontradas no forman parte del Código Procesal Penal Federal de Brasil, sino que gran parte de las medidas identificadas, en realidad forman parte de su famosa normativa del Marco Civil de Internet (Ley Federal Nº. 12.965/2014), que paradójicamente, aunque habla de un marco civil y no penal, su regulación incluye obligaciones legales que terminan siendo aprovechadas por el sistema penal.

De las 5 medidas de investigación que han podido detectarse, 3 se encontraron en la Ley de Marco Civil de Internet antes citada, y 2, relacionadas a las interceptación de comunicaciones, se han detectado dentro de la normativa N° 9.296, que si bien es originalmente del año 1996, ha tenido una importante actualización en 2019 a través del anormativa Nº 13.964.

De esta forma, Brasil ha regulado 5 de las 6 medidas de investigación “básicas” sugeridas por el Convenio de Budapest, sin tener ningún tipo de regulación sobre las medidas más modernas que hemos incluído en el estudio. Por esta razón, el bajo nivel de cumplimiento ha dejado a este importante país en el 7mo. lugar en el ranking elaborado en la Tabla Nº 38, logrando estar por encima sólo de CABA (Argentina) y el fuero federal argentino.

En relación al caso colombiano no hemos encontrado grandes sorpresas. Como se ha podido ver a lo largo del estudio, Colombia no posee una regulación específica sobre medidas de investigación y evidencia digital, sino que hemos detectado una breve regulación dentro de su Código Procesal Penal, con una regulación algo difusa y con una terminología que no termina de acomodarse a los estándares internacionales.

Debemos comenzar diciendo que en Colombia hemos encontrado reguladas 4.5 medidas de las 6 básicas, indicando ese valor toda vez que en una no quedamos convencidos que pueda aplicarse adecuadamente, por lo que hemos considerado que el art. 244 en parcialmente aplicable al caso de conservación y divulgación inmediata de datos de tráfico.

La novedad es que, por fuera de esta regulación básica, Colombia ha regulado la figura especial del Agente Encubierto Informático o Digital, siendo una de los institutos modernos dentro de la investigación. Es importante señalar que la regulación de dicha figura ha sido incorporada en el año 2018, a través de la Ley Nº 1908, dedicada a "fortalecer la investigación y judicialización de organizaciones criminales", con una clara finalidad de cooperar en la lucha histórica que tienen contra bandas de narcotráfico y grupos paramilitares dentro del país.

A nivel general, Colombia entonces ha registrado un nivel de cumplimiento de 41,67% de medidas reguladas y un 8,33% de medidas parcialmente reguladas, dejando al país cafetero en el sexto lugar en el ranking de la Tabla Nº 38.

En relación al caso mexicano cabe realizar una advertencia en relación al alcance del estudio, dejando constancia que sólo se ha revisado la normativa procesal penal a nivel federal, sin acceder a una búsqueda pormenorizada en los distintos estados mexicanos. Quizás, de la misma forma que hemos observado en Argentina, algunos Estados Mexicanos poseen actualmente buenos niveles de regulación al respecto, pero los límites metodológicos fijados nos han impedido poder realizar dicha comprobación.

Realizada esta disquisición, la regulación en el Código Procesal Federal Mexicano tampoco nos ha dado demasiadas sorpresas. Dentro del esquema básico de las medidas de investigación, si bien podríamos afirmar que se han encontrado medidas aplicables a los seis casos, hemos considerado que tanto el mandato de comunicación, así como el registro y decomiso de datos informáticos almacenados no están adecuadamente regulados, por lo que hemos considerado que las figuras reguladas son parcialmente aplicables.

La novedad en México, viene de la mano de la regulación del art. 295, con una regulación bastante clara en relación al caso de advertir un hallazgo casual en el marco de una intervención de comunicaciones. Si bien no da demasiada información al respecto, ni tampoco hace referencias a comunicaciones electrónicas en sí, lo cierto es que al mencionar "intervención de comunicaciones privadas" hemos considerado (teniendo un criterio de interpretación amplio y amigable), que tranquilamente podría aplicarse al caso de las comunicaciones electrónicas.

Gracias a esta regulación, México ha logrado escalar a la 4ta posición de nuestro ranking de la Tabla Nº 38, contando con un 41,67% de medidas adecuadamente reguladas y un 16,67% de medidas parcialmente reguladas.

De esta forma, llegamos al último país alcanzado por el estudio, España, que también ha quedado en este lugar por una cuestión estratégica, toda vez que previo a la realización de la investigación concreta, ya podíamos presumir del buen nivel de este país europeo, que fue intencionalmente seleccionado como parte del alcance, para tener un punto de comparación que no fuera latinoamericano.

España ha confirmado su buen nivel en materia procesal penal, quedando en un segundo lugar con un 75% de nivel de cumplimiento, sumado a un 8,33% de cumplimiento parcial, toda vez que hemos considerado que su regulación sobre los hallazgos casuales, sólo refieren a la correspondencia escrita y telegráfica, lo que hace que su interpretación sea mucho más restrictiva que la que hemos explicado previamente para el caso mexicano.

Con respecto al caso español se puede afirmar un punto extra a favor por su minuciosidad al momento de la regulación, un aspecto que no hemos calificado, toda vez que desde el punto de vista metodológico habría sido una complejidad mayor a la que ya nos representó el estudio. De todas maneras, destacamos que la rigurosidad española es digna de ser valorada, toda vez que su articulado no es una mera enunciación y habilitación genérica, sino que se observa la existencia de una verdadera preocupación con respecto a los límites y controles que deben ser realizados en la ejecución de la misma.

En relación a las figuras de mayor novedad que hemos encontrado, dejando de lado el agente encubierto informático y el registro remoto, podemos destacar la inclusión de regulación sobre el acceso transfronterizo de datos y algo que hemos considerado como parcialmente aplicable para los hallazgos casuales que involucren algún tipo de evidencia digital.

Adicionalmente, hacemos mención especial para el caso de la regulación de la posibilidad de utilización de técnicas que permitan el acceso a datos necesarios para la identificación de un usuario / dispositivo / conexión (art. 588 ter k, 588 ter i y 588 ter m). Esta figura, es lo más cercano que hemos encontrado a la técnica especial de investigación desarrollados en la sección 6.3.4. de esta tesis, referida a la técnica de identificación de dispositivo por Browser fingerprinting (como una de las posibles).

España ha validado entonces continuar siendo una referencia para la normativa Latinoamericana, con su mayor nivel de madurez en la materia, producto de tener más años trabajando sobre la materia.

7.9. Conclusiones sobre las medidas de investigación reguladas

Que, de acuerdo a lo observado en la Tabla Nº 40, es posible concluir con que las primeras seis medidas de investigación más reguladas de todo el estudio, coinciden con las medidas de investigación sugeridas por el Convenio de Cibercrimen de Budapest (y ahora también, por el Proyecto de ONU).

Que, dentro de ese primer grupo de medidas, la intercepción de datos relativos al contenido ha sido la más regulada, logrando casi un 89% de regulación en los países del estudio. Entendemos que la explicación sobre ello tiene que ver con que, previa a la llegada del cibercrimen en todo su esplendor, en el delito clásico, la intervención de comunicaciones siempre fue una de las medidas estrella, por lo que su adaptación en algunos casos, ni siquiera fue necesaria (ya que el concepto de comunicación era lo suficientemente amplia como para incluir a las electrónicas).

En segundo lugar con un 77,78% se observa al registro y decomiso de datos informáticos almacenados, otra de las medidas con un fuerte parentesco con las medidas tradicionales de las figuras que llevan su nombre.

Que, compartiendo el tercer y cuarto lugar, con el mismo porcentaje de 66,67% (y un 11,11% parcialmente regulado) encontramos el mandato de comunicación y la conservación inmediata de datos de tráfico. Comenzando por el mandato de comunicación podemos afirmar que se trata de otra figura que de alguna forma también ya existía, toda vez que la fiscalía siempre había tenido la posibilidad de requerir la cooperación -forzada- de los privados, aunque en muchos casos, esa posibilidad estaba regulada en las propias normativas orgánicas de los Ministerios Públicos Fiscales, y no tanto en el propio Código Procesal Penal, quizás por no haber tanto consenso acerca de si era o no una medida de injerencia.

Que, en relación a la conservación y divulgación de datos de tráfico, así como con la medida de recolección en tiempo real de datos de tráfico (que ocupa el 5to lugar con un 66,67%) entendemos que son figuras históricamente utilizadas por las fiscalías y fuerzas de seguridad. Por un lado, era a través de la solicitud de las tan conocidas “listas sábanas” de llamadas telefónicas, que no eran otra cosa que los datos de tráfico de las comunicaciones telefónicas. Por otro lado, la recolección en tiempo real, que siempre fue menos utilizado en las comunicaciones clásicas toda vez que a diferencias de las electrónicas, sobre las telefónicas siempre quedaba registro de tráfico de las mismas, ya que era la información necesaria para luego realizar la correspondiente facturación al cliente.

Que, como sucedía con el mandato de comunicación, el acceso a la información de tráfico por lo general tenía por fundamento normativa interna de la propia fiscalía (en el caso que sea un o una fiscal quien ordenara dicha información), toda vez que en muchas jurisdicciones argentinas, aún dicha información es solicitada directamente por la policía local, sin ningún tipo de cuestionamientos al respecto. Este -como otros tantos casos- dejan a la luz la importancia para todos estos casos, de la existencia de una normativa clara que determine quién puede solicitar esa información y bajo qué requisitos.

Que, en sexto lugar encontramos a la conservación inmediata de datos informáticos almacenados, que de todas las medidas sugeridas por el Convenio de Cibercrimen de Budapest, es la menos relacionada o emparentada con otras medidas de investigación utilizadas en la investigación de los delitos clásicos. ¿Será este motivo la razón por la cuál es una de las menos reguladas -dentro de esta gama de medidas sugeridas internacionalmente-? No es posible realizar tal afirmación, pero sí podemos dejar esta opción como una de las hipótesis posibles que de explicación sobre su bajo nivel de regulación a nivel procesal penal.

Que, tratando de optar por una mirada de optimismo y a modo de dato estadístico, puede concluirse que de las medidas sugeridas internacionalmente, en los países incluídos por el estudio (y sus respectivas jurisdicciones alcanzadas), todas se encontraron como mínimo, con un nivel del 66,67% de regulación, evidenciando un nivel de regulación “aceptable”. Sin embargo, si nos ponemos más finos con las estadísticas y números, podemos observar que de ese primer grupo de 6 medidas más reguladas, sólo las dos primeras (interceptación de datos de contenido y registro y decomiso de datos informáticos) poseen una regulación superior al 70%.

Que, si decidimos tener una lectura más exigente en relación a la importancia que tiene para salvaguardar los derechos y garantías de las personas, que las medidas de injerencia que aplique el Estado, se encuentren reguladas, observar que 4 de las 6 medidas más importantes y con sugerencia internacional, se encuentran con un 66% de cumplimiento (algunos con un poquito más de regulación parcial), el optimismo se va diluyendo, demostrando que el camino que falta recorrer en materia procesal penal aún es importante.

Que, en la segunda mitad de la Tabla Nº 40, encontramos lógicamente las restantes seis medidas que hemos incorporado al estudio, pero sobre las que aún no existe un claro consenso internacional acerca de su regulación, o al menos, en algunas más que en otras pero ninguna aún llegado a ese nivel. Que, las seis medidas de este segundo grupo, se encontraron por debajo del 50% de regulación en las jurisdicciones analizadas por esta tesis.

Que, la prueba de la falta de consenso internacional puede observarse en las discusiones actuales que existen en torno al Proyecto de la Convención Internacional Integral sobre la Lucha contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos, que en el año 2024 aún sigue insistiendo con las medidas de investigación que el Convenio de Cibercrimen de Budapest ya había esbozado en el año 2000.

Que, en esta segunda mitad de la tabla, vemos en primer lugar (con un 44,44% de regulación) quizás a la medida que mayor nivel de aceptación tiene a nivel internacional, y sobre la cuál se puede encontrar amplia doctrina e incluso algunos casos de jurisprudencia sobre la misma. Nos referimos a la figura del agente encubierto informático o digital, una figura no tan novedosa desde el punto de vista penal, toda vez que el agente encubierto clásico lleva muchos años de vida en el ámbito de la investigación, y en este caso, sería la adaptación de dicha figura al nuevo mundo digital.

Que, esta medida regulada -dentro de los países alcanzados por nuestro estudio- en Argentina (Mendoza y Salta), Colombia y España, se puede encontrar con diferentes formas de regulación. Las más completas son las nuevas figuras argentinas del caso de Mendoza y Salta, que no sólo han sido reguladas como medidas independientes, sino con un alto nivel de detalle. En Colombia, si bien es una figura independiente, su regulación es más bien escasa (en comparación con todos los aspectos que deberían haberse tenido en cuenta).

Que, España ha sido el país que cronológicamente hablando dentro de nuestro estudio, fue el primero en regular el agente encubierto informático, y que decidió no generar una figura independiente sino que optó por incluirla dentro de la regulación de la medida clásica del agente encubierto, como si fuera un subgénero de la misma, aplicando a la misma todas las limitaciones y requisitos que son necesarias para la figura madre.

Que, en octavo lugar, con un 33,33% de regulación encontramos probablemente a otra de los institutos sobre los que más se puede encontrar -actualmente- artículos de doctrina y discusiones al respecto, incluso en el marco de congresos y eventos de la materia: el registro remoto.

Qué, de las 3 jurisdicciones donde se ha regulado la figura (España, y Mendoza y Salta en Argentina), Mendoza ha sido la que posee una regulación más breve, y a nuestro criterio, insuficiente. Si bien hemos dudado en clasificar esta figura en Mendoza como parcialmente aplicable, ya que como explicamos en el desarrollo de la tesis, parece ser más que habilita a una extracción remota de datos en el marco de un registro domiciliario que a un registro remoto sin conocimiento del titular o propietario del sistema o dispositivo, finalmente hemos optado por tener un criterio de interpretación amplio, en vistas de las posibilidades de regulación provincial.

En esta figura, nuevamente las dos ganadoras del estudio (España y Salta) se llevan el premio a la mejor regulación, con una regulación detallada y organizada. Destacamos la diferencia que en el caso de España, el registro remoto sólo podrá aplicarse para delitos concretos, cuando en cambio en Salta, se hace mención de casos de delitos con "especial gravedad", cuya habilitación quedará sujeta a la decisión judicial de turno.

En los últimos 4 puestos de la Tabla Nº 40 con el ranking de niveles de regulación de las medidas, encontramos a quizás 4 de los institutos más cuestionados o debatidos. En noveno lugar encontramos a los hallazgos casuales en evidencia digital, con un 22,22% (más un 11,11% de parcialmente regulado) de cumplimiento. Una figura que estaríamos de acuerdo en que técnicamente, no sería una medida o técnica de investigación sobre evidencia digital, pero que sí se trata de un instituto históricamente discutido (plain view) cuya adaptación al nuevo mundo virtual también ha traído gran caudal de opiniones y cuestionamientos.

A nuestro criterio, la mejor regulación de esta figura se ha encontrado en la normativa salteña, incluída en el art. 309 quater, con una sencilla pero contundente obligación de comunicar los datos hallados al Juez de Garantías, y sosteniendo su validez siempre y cuando hayan sido encontrados de manera casual en cumplimiento y siguiendo los parámetros y requisitos establecidos en la orden judicial original.

Que, como hemos explicado al momento de la construcción de las categorías nos pareció de interés incluir tanto este instituto como el desbloqueo compulsivo de

datos, el acceso transfronterizo de datos y el OSINT, toda vez que a nuestro criterio, si bien el más cercano a una técnica de investigación es OSINT y desbloqueo compulsivo de datos informáticos, tanto el acceso transfronterizo de datos como el caso de los hallazgos casuales son, a nuestro criterio, fundamentales para cualquier sistema procesal penal que tenga intenciones de lograr coherencia y eficacia en el marco de la investigación del cibercrimen.

Somos conscientes que su inclusión no ha sido sencilla, y de sus posibles cuestionamientos desde el punto de vista de la asepsia metodológica que toda investigación debe tener, no obstante, estamos orgullosos de poder haberlos incluídos en el estudio, dando cuenta de institutos sobre los que tampoco existen (o al menos no hemos encontrado) estudios al respecto que puedan dar cuenta de su regulación en el derecho comparado (si por supuesto, existen aquellos que lo abordan desde otras ópticas).

Que, en décimo lugar de nuestro ranking encontramos al acceso transfronterizo de datos, uno de los institutos más importantes en materia procesal penal, y sin embargo, con una regulación de sólo el 22,22% de acuerdo a nuestro estudio. Nuevamente, las únicas jurisdicciones con regulación al respecto han sido Salta (Argentina) y España, casualmente las dos jurisdicciones que han liderado el estudio.

Que, de la diferencia de regulación entre ambos, destacamos la postura que ha tenido en cuenta el Comité especializado que generó la normativa salteña, donde casualmente se encontraba el Dr. Marcos Salt, especialista en la temática, donde se ha optado por incluir un inciso c, que habilita el acceso transfronterizo de datos cuando no resulte posible determinar en forma certera, al momento de ejecución de la medida, la jurisdicción en la cual los datos están alojados.

Que, reiteramos nuestra celebración a este tipo de iniciativas que se animan a proponer algo diferente, ya que habilita con un argumento técnico (la falta de certeza de la ubicación de los datos) la apertura a una puerta al acceso transfronterizo de datos sobre la que, incluso a nivel internacional, existe tanta reticencia para su regulación. Hasta podríamos decir que su incorporación es estratégica, toda vez que su regulación a nivel “local” en una Provincia Argentina hace que llame menos la

atención que si la misma regla fuera regulada en el marco del Código Procesal Penal Federal.

En el puesto 11 con un 0% de regulación y un 11% de regulación parcial, encontramos al tan conocido pero poco regulado uso del OSINT, que si bien en muchos lugares puede ser encontrado como un tipo de inteligencia tradicional, consideramos que de la misma forma que la regulación sobre otros institutos deben ser adecuados al mundo digital, aquí también dejamos constancia de la importancia de regulación sobre una técnica que se utiliza casi a diario por las fuerzas de seguridad.

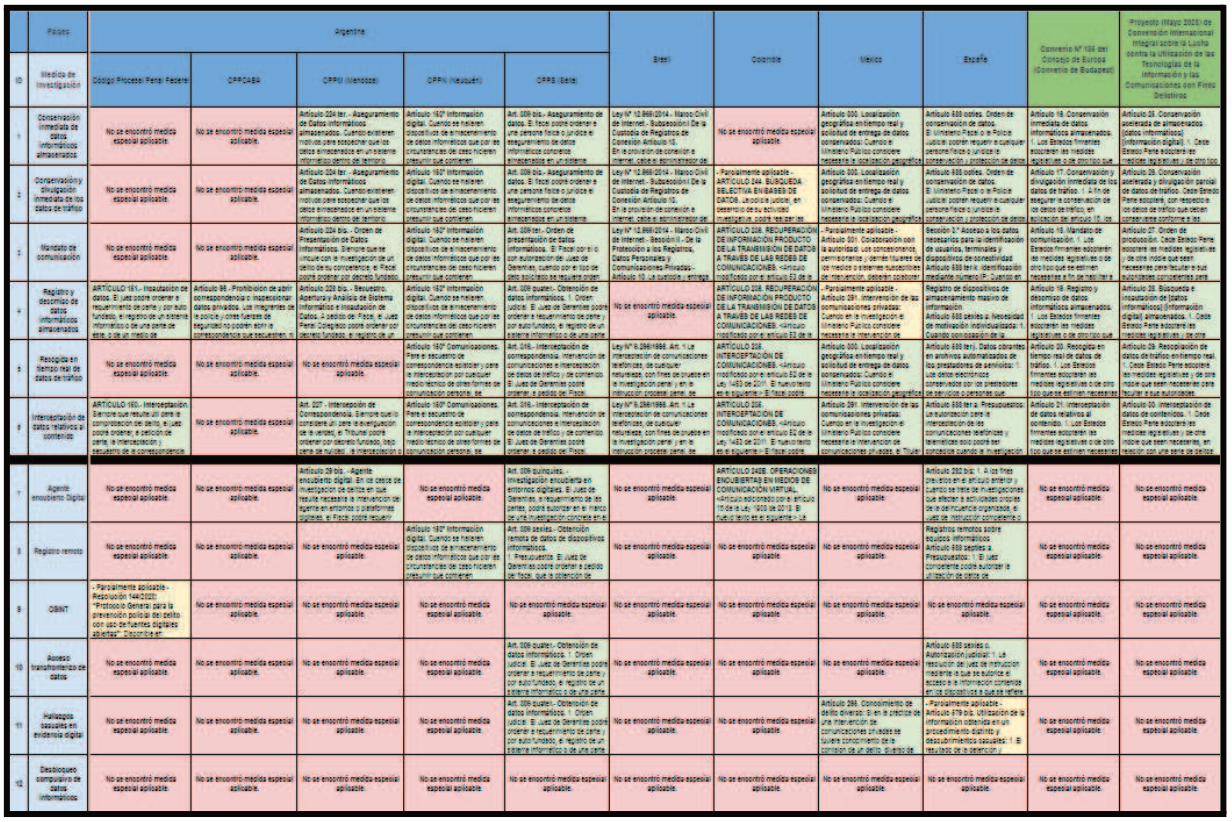
Que, si bien el OSINT ha sido normalmente vinculado a tareas de prevención de seguridad, también es muy utilizado para la generación de informes de inteligencia criminal en el marco de investigaciones de hechos ya consumados.

Que, el único caso de regulación parcial que hemos encontrado, ha sido en Argentina a nivel nacional, con una muy interesante normativa destinada a la regulación de tareas de prevención en el marco de la situación de emergencia por el COVID-19.

Que, como hemos desarrollado a lo largo de nuestra tesis, aunque prima facie parece que el hecho que la información se encuentre en fuentes abiertas implica que no sea necesaria su regulación, desde nuestro punto de vista consideramos que si se hace necesaria. Que, existen casos concretos analizados en este trabajo, que demuestran que un uso abusivo de esta técnica, también puede terminar con la afectación de derechos y salvaguardas de las personas.

Que, en último lugar, con ningún nivel de regulación al respecto, encontramos al desbloqueo compulsivo de datos informáticos, otro de los grandes tópicos que adeudamos como desafío en la materia, en un contexto tecnológico donde el cifrado es cada vez más utilizado en infinidad de dispositivos y sistemas, y donde -al menos para el momento de escribir estas líneas- la tecnología de los laboratorios forenses se encuentra limitada para forzar el acceso a los datos que se encuentran almacenados en dichos dispositivos.

Para finalizar, nos parece adecuado comenzar brindar un repaso del panorama general del estudio realizado, a fin de destacar una de las primeras conclusiones de relevancia para este trabajo.



ID	País	Argentina					Brasil	Colombia	México	España	Convenio Nº 185 del Consejo de Europa (Convenio de Budapest)	Proyecto (Mayo 2023) de Convención Internacional integral sobre la Lucha contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos
	Medida de investigación	Código Procesal Penal Federal	CPPCABA	CPPN (Mendoza)	CPPN (Neuquén)	CPPBS (Salta)						
1	Conservación inmediata de datos informáticos almacenados	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	Artículo 224 ter.- Aseguramiento de Datos Informáticos almacenados. Cuando existieren motivos para sospechar que los datos almacenados en un sistema informático dentro de territorio	Artículo 183º Información digital. Cuando se hallaren dispositivos de almacenamiento de datos informáticos que por las circunstancias de caso hiciere presumir que contienen	Art. 309 bis.- Aseguramiento de datos. El fiscal podrá ordenar a una persona física o jurídica el aseguramiento de datos informáticos concretos almacenados en un sistema	Ley Nº 12.965/2014 - Marco Civil de Internet - Subsección I De la Custodia de Registros de Conexión Artículo 13. En la provisión de conexión a internet, cabe a administrador de	No se encontró medida especial aplicable.	Artículo 333. Localización geográfica en tiempo real y solicitud de entrega de datos conservados: Cuando el Ministerio Público considere necesaria la localización geográfica	Artículo 588 octies. Orden de conservación de datos. El Ministerio Fiscal o la Policía Judicial podrán requerir a cualquier persona física o jurídica la conservación y protección de datos	Artículo 16. Conservación inmediata de datos informáticos almacenados. 1. Las Estados Firmantes estudiarán las medidas legislativas que sean	Artículo 29. Conservación acelerada de almacenados [datos informáticos] [información digital]. 1. Cada Estado Parte adoptará las medidas legislativas y de otro tipo
2	Conservación y divulgación inmediata de los datos de tráfico	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	Artículo 224 ter.- Aseguramiento de Datos Informáticos almacenados. Cuando existieren motivos para sospechar que los datos almacenados en un sistema informático dentro de territorio	Artículo 183º Información digital. Cuando se hallaren dispositivos de almacenamiento de datos informáticos que por las circunstancias de caso hiciere presumir que contienen	Art. 309 bis.- Aseguramiento de datos. El fiscal podrá ordenar a una persona física o jurídica el aseguramiento de datos informáticos concretos almacenados en un sistema	Ley Nº 12.965/2014 - Marco Civil de Internet - Subsección I De la Custodia de Registros de Conexión Artículo 13. En la provisión de conexión a internet, cabe a administrador de	- Parcialmente aplicable - ARTICULO 244. BUSQUEDA SELECTIVA EN BASES DE DATOS. Un juez de instrucción, en desarrollo de su actividad investigativa, podrá ser parte de	Artículo 333. Localización geográfica en tiempo real y solicitud de entrega de datos conservados: Cuando el Ministerio Público considere necesaria la localización geográfica	Artículo 588 octies. Orden de conservación de datos. El Ministerio Fiscal o la Policía Judicial podrán requerir a cualquier persona física o jurídica la conservación y protección de datos	Artículo 17. Conservación y divulgación inmediata de los datos de tráfico. 1. A fin de asegurar la conservación de los datos de tráfico, en aplicación del artículo 16, las	Artículo 29. Conservación acelerada y divulgación parcial de datos de tráfico. Cada Estado Parte adoptará, con respecto a los datos de tráfico que deben conservarse conforme a las
3	Mandato de comunicación	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	Artículo 224 bis.- Orden de Presentación de Datos Informáticos. Siempre que se ordene con la investigación de un delito de su competencia, el Fiscal podrá ordenar por decreto fundado,	Artículo 183º Información digital. Cuando se hallaren dispositivos de almacenamiento de datos informáticos que por las circunstancias de caso hiciere presumir que contienen	Art. 309 bis.- Orden de presentación de datos informáticos. El Fiscal podrá o hacer con la investigación de un delito de su competencia, el Fiscal podrá ordenar por decreto fundado,	Ley Nº 12.965/2014 - Marco Civil de Internet - Sección II - De la Protección a los Registros, Datos Personales y Comunicaciones Privadas - Artículo 10. La custodia, entrega	ARTÍCULO 224. REQUERIMIENTO DE INFORMACIÓN PRODUCTO DE LA TRANSMISIÓN DE DATOS A TRAVÉS DE LAS REDES DE COMUNICACIONES. «Artículo modificado por el artículo 53 de la	- Parcialmente aplicable - Artículo 591. Colaboración con la autoridad. Los concesionarios, permisionarios y demás titulares de los medios o sistemas susceptibles de intervención, deberán colaborar	Sección 3.ª Acceso a los datos necesarios para la identificación de usuarios, terminales y dispositivos de conectividad. Artículo 588 ter k. Identificación mediante número IP. Cuando en	Artículo 18. Mandato de comunicación. 1. Las Estados Firmantes adoptarán las medidas legislativas que sean necesarias para facultar a las	Artículo 27. Orden de producción. Cada Estado Parte adoptará las medidas legislativas y de otro índole que sean necesarias para facultar a sus autoridades competentes para
4	Registro y desarmo de datos informáticos almacenados	ARTÍCULO 181.- Inspección de cosas. El juez podrá ordenar a requerimiento de parte y por auto fundado, el registro de un sistema informático o de una parte de éste, o de un medio de	Artículo 96.- Prohibición de abrir correspondencia o inspeccionar datos privados. Los integrantes de la policía y otras fuerzas de seguridad no podrán abrir o correspondencia que secuestren, a	Artículo 228 bis.- Resguardo, Apertura y Análisis de Sistema Informático e Incautación de Datos. A pedido del Fiscal, el Juez Penal Colegiado podrá ordenar por decreto fundado, el registro de un	Artículo 183º Información digital. Cuando se hallaren dispositivos de almacenamiento de datos informáticos que por las circunstancias de caso hiciere presumir que contienen	Art. 309 quater.- Obtención de datos informáticos. 1. Orden judicial. El juez de Garantías podrá ordenar a requerimiento de parte y por auto fundado, el registro de un sistema informático o de una parte	No se encontró medida especial aplicable.	ARTÍCULO 224. REQUERIMIENTO DE INFORMACIÓN PRODUCTO DE LA TRANSMISIÓN DE DATOS A TRAVÉS DE LAS REDES DE COMUNICACIONES. «Artículo modificado por el artículo 53 de la	- Parcialmente aplicable - Artículo 591. Intervención de las comunicaciones privadas: Cuando en la investigación el Ministerio Público considere necesaria la intervención de	Registro de dispositivos de almacenamiento masivo de información Artículo 588 sexies a. Necesidad de motivación individualizada. 1. Cuando con ocasión de la	Artículo 19. Registro y desarmo de datos informáticos almacenados. 1. Las Estados firmantes adoptarán las medidas legislativas que sean	Artículo 28. Búsqueda e inquisición de [datos informáticos] [información digital] almacenados. 1. Cada Estado Parte adoptará las medidas legislativas que sean
5	Recogida en tiempo real de datos de tráfico	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	Artículo 183º Comunicaciones. Para el secuestro de correspondencia epistolar y para la interceptación por cualquier medio técnico de otras formas de comunicación personal, se	Art. 240.- Interceptación de correspondencia. Intervención de comunicaciones e interceptación de datos de tráfico y de contenido. El juez de Garantías podrá ordenar, a pedido del Fiscal	Ley Nº 9.296/1996. Art. 1.º La interceptación de comunicaciones telefónicas, de cualquier naturaleza, con fines de prueba en la investigación penal y en la instrucción procesal penal, se	ARTÍCULO 228. INTERCEPTACIÓN DE COMUNICACIONES. «Artículo modificado por el artículo 53 de la Ley 1453 de 2011. El nuevo texto es el siguiente:» El fiscal podrá	Artículo 333. Localización geográfica en tiempo real y solicitud de entrega de datos conservados: Cuando el Ministerio Público considere necesaria la localización geográfica	Artículo 588 ter j. Datos obrantes en archivos automatizados de los prestadores de servicios. 1. Los datos electrónicos conservados por los prestadores de servicios o personas que	Artículo 20. Recogida en tiempo real de datos de tráfico. 1. Las Estados firmantes adoptarán las medidas legislativas que sean necesarias para facultar a sus autoridades	Artículo 29. Recopilación de datos de tráfico en tiempo real. 1. Cada Estado Parte adoptará las medidas legislativas y de otro tipo que sean necesarias para
6	Intercepción de datos relativos al contenido	ARTÍCULO 150.- Interceptación. Siempre que resulte útil para la comprobación de delito, el juez podrá ordenar, a petición de parte, la interceptación y secuestro de la correspondencia	No se encontró medida especial aplicable.	Art. 227.- Intercepción de Correspondencia. Siempre que lo considere útil para la averiguación de la verdad, el Tribunal podrá ordenar por decreto fundado, bajo pena de nulidad, la interceptación o	Artículo 183º Comunicaciones. Para el secuestro de correspondencia epistolar y para la interceptación por cualquier medio técnico de otras formas de comunicación personal, se	Art. 236.- Interceptación de correspondencia. Intervención de comunicaciones e interceptación de datos de tráfico y de contenido. El juez de Garantías podrá ordenar, a pedido del Fiscal	Ley Nº 9.296/1996. Art. 1.º La interceptación de comunicaciones telefónicas, de cualquier naturaleza, con fines de prueba en la investigación penal y en la instrucción procesal penal, se	ARTÍCULO 228. INTERCEPTACIÓN DE COMUNICACIONES. «Artículo modificado por el artículo 53 de la Ley 1453 de 2011. El nuevo texto es el siguiente:» El fiscal podrá	Artículo 588 ter a. Presupuestos. La autorización para la interceptación de las comunicaciones telefónicas y telemáticas sólo podrá ser concedida cuando la investigación	Artículo 21. Interceptación de datos relativos al contenido. 1. Las Estados firmantes adoptarán las medidas legislativas que sean necesarias, en relación con una serie de	Artículo 30. Interceptación de datos de contenidos. 1. Cada Estado Parte adoptará las medidas legislativas que sean necesarias, en relación con una serie de delitos
7	Agente encubierto Digital	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	Artículo 29 bis.- Agente encubierto digital. En los casos de investigación de delitos en que resulte necesaria la intervención de agentes encubiertos o usuarios encubiertos en entornos digitales, el Fiscal podrá requerir	No se encontró medida especial aplicable.	Art. 309 quinquies.- Investigación encubierta en entornos digitales. El Juez de Garantías, a requerimiento de las partes, podrá autorizar en el marco de una investigación concreta en el	No se encontró medida especial aplicable.	ARTÍCULO 242B. OPERACIONES ENCUBIERTAS EN REDES DE COMUNICACIÓN VIRTUAL. «Artículo adicionado por el artículo 15 de la Ley 1908 de 2018. El nuevo texto es el siguiente:» La	No se encontró medida especial aplicable.	Artículo 282 bis. 1. A los fines previstos en el artículo anterior y cuando se trate de investigaciones que afecten a actividades propias de la delincuencia organizada, el juez de instrucción competente o	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.
8	Registro remoto	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	Artículo 183º Información digital. Cuando se hallaren dispositivos de almacenamiento de datos informáticos que por las circunstancias de caso hiciere presumir que contienen	Art. 309 sexies.- Obtención remota de datos de dispositivos informáticos. 1. Procedencia. El Juez de Garantías podrá ordenar a pedido del Fiscal, que la obtención de	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	Registros remotos sobre equipos informáticos. Artículo 588 septies a. Presupuestos. 1. El juez competente podrá autorizar la utilización de datos de	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.
9	OSINT	- Parcialmente aplicable - Resolución 144/2020: "Protocolo General para la prevención policial del delito con uso de fuentes digitales abiertas". Establece el	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.
10	Acceso transfronterizo de datos	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	Art. 309 quater.- Obtención de datos informáticos. 1. Orden judicial. El juez de Garantías podrá ordenar a requerimiento de parte y por auto fundado, el registro de un sistema informático o de una parte	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	Artículo 588 sexies c. Autorización judicial. 1. La resolución del juez de instrucción mediante la que se autorice el acceso a la información contenida en los dispositivos a que se refiere	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.
11	Hallazgos casuales en evidencia digital	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	Art. 309 quater.- Obtención de datos informáticos. 1. Orden judicial. El juez de Garantías podrá ordenar a requerimiento de parte y por auto fundado, el registro de un sistema informático o de una parte	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	Artículo 286. Conocimiento de delito diverso. Si en la práctica de una intervención de comunicaciones orales se tuviere conocimiento de la comisión de un delito diverso de	- Parcialmente aplicable - Artículo 879 bis. Utilización de la información obtenida en un procedimiento distinto y descubrimientos casuales. 1. El resultado de la detención y	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.
12	Desbloqueo compulsivo de datos informáticos	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.	No se encontró medida especial aplicable.

Tabla Nº 34: Cuadro general comparativo del estudio de derecho comparado sobre medidas de investigación reguladas en los países alcanzados por el estudio

Varias conclusiones podemos destacar de dicho cuadro, comenzando por advertir que, como hemos explicado en la sección 7.1.1. (Tabla Nº 25), del listado de medidas o técnicas de investigación seleccionadas como alcance para nuestro trabajo, teníamos claro previo a comenzar que las primeras 6 medidas eran las sugeridas internacionalmente por el Convenio de Cibercrimen de Budapest (y que también son las mismas consideradas por parte de la ONU en su actual proyecto), y el resto de las medidas (desde la Nº 7 a la Nº 12) eran medidas más novedosas o disruptivas.

La primera conclusión que puede observarse recurriendo a los resultados de la Tabla Nº 39, es precisamente que, de las medidas recomendadas a nivel

internacional, se encuentra un mayor nivel de regulación en los sistemas procesales penales, donde todas las medidas tienen como mínimo un 66,67%, llegando la más regulada (interceptación de comunicaciones) a estar en el nivel del 88,89% de regulación.

De dicha línea hacia abajo, las medidas de investigación son quizás aquellas más disruptivas o novedosas, donde hemos concentrado: al agente encubierto informático o digital, el registro remoto, la práctica de OSINT, el acceso transfronterizo de datos, los hallazgos casuales en evidencia digital y el desbloqueo compulsivo de datos.

Como se puede observar a simple vista, esas medidas de investigación son las menos encontradas, y quizás donde exista el mayor nivel de ausencia normativa, al menos en los países incluídos en el presente estudio.

Capítulo VIII: Conclusiones

Luego de todo el desarrollo realizado, estamos en consideración de proceder a la generación de las respuestas formales sobre las hipótesis de trabajo planteadas.

8.1. Hipótesis 1: ¿Están adecuadamente tipificados los delitos informáticos?

La primera de las hipótesis planteada en nuestra tesis, postulaba que "*a nivel de normativa penal material, los países latinoamericanos han adecuado sus ordenamientos jurídicos para tipificar los delitos informáticos sugeridos por el Convenio de Budapest (art. 2 a 9)*".

De acuerdo a lo observado en la Tabla Nº 17a, donde se ha tenido en cuenta exclusivamente los tipos penales sugeridos internacionalmente por el Convenio de Cibercrimen de Budapest, todos los países incluídos en el estudio oscilaron entre el 75% y el 87,5% de los tipos penales adecuadamente tipificados, con un nivel de entre 12,5% y el 25% del resto de los delitos, al menos parcialmente tipificados.

De acuerdo a estos índices, consideramos que estamos en condiciones de afirmar que, de acuerdo a la hipótesis elaborada, al momento de realizar el presente estudio, tanto Argentina, Brasil, Colombia, México como España, posee sus ordenamientos jurídicos adecuados en relación a la tipificación de los delitos informáticos sugeridos por el Convenio de Cibercrimen de Budapest.

Reiteramos que a nivel general podemos afirmar que de la totalidad de delitos seleccionados para formar parte de este estudio, los que estadísticamente se encuentran más regulados, coinciden con aquellos que la Convención de Cibercrimen de Budapest considera como obligatorios para los Estados adheridos. De la Tabla Nº 19 puede observarse que los primeros seis delitos con mayor nivel de tipicidad, son precisamente aquellos pertenecientes al listado propuesto por dicho Convenio.

Por lo expuesto y al momento de la redacción de estas líneas (Marzo 2024), estamos en condiciones de afirmar que la mayoría de los países incluídos en el estudio se encuentran en un nivel de cumplimiento adecuado en relación a los delitos informáticos sugeridos por el Convenio de Budapest.

En otro orden y relacionado con los aspectos interpretativos que toda investigación tiene, aclaramos que no sería correcto considerar que los resultados expuestos permiten concluir que técnicamente un país determinado se encuentra o no en cumplimiento de las disposiciones en materia penal que dispone la Convención de Cibercriminalidad de Budapest, toda vez que si bien gran parte de las figuras penales consideradas han sido tomadas de la Sección 1 sobre Materia Penal de esta Convención, ello no implica que se ha hecho un análisis pormenorizado de todos los requisitos que se establecen en cada artículo penal de este instrumento jurídico internacional.

Es decir, si bien es posible que los resultados arrojados por el estudio indiquen una tendencia o aproximación de dicho país sobre la situación penal material en relación a los delitos informáticos en relación a la Convención de Budapest ello no permite deducir que dicho país cumpla o no con los requisitos de la Convención, tarea que no ha sido objeto de la presente investigación. En adhesión a lo expuesto, debe recordarse que se ha excluido de dicho análisis el estudio del art. 10 sobre infracciones relativas al contenido, en especial a la propiedad intelectual, que hubiese implicado el estudio de todo un complejo campo jurídico como es el que regula la propiedad intelectual.

Que, entendemos que los resultados publicados expresan con claridad la existencia de normativa material penal en relación a los delitos informáticos básicos considerados por el Convenio de Cibercrimen de Budapest, pudiendo descartarse la hipótesis acerca de que la “inexistencia” o “laguna jurídica” existente en la materia pueda considerarse como una de las responsables de la falta de eficacia existente (de acuerdo a lo estudiado en el Capítulo III) en relación a la lucha contra el cibercrimen.

Que, no obstante la afirmación realizada, se deja constancia del potencial desafío que representa la incorporación de figuras penales específicas para perseguir determinadas conductas disvaliosas que quedaron por fuera del Convenio

de Budapest, como se puede observar de acuerdo al estudio, sucede con las conductas de violación de datos personales, suplantación de identidad digital y captación ilegítima de datos confidenciales (phishing).

Que, dejamos constancia de que, de acuerdo al estudio realizado en la sección 4.5.2, ninguno de los países poseía una regulación especial en materia de tipificación de los delitos informáticos, encontrándose en todos los casos normativas de actualización que han modificado o aggiornado sus propias normas penales para agregar, en mayor o menor medida según el resto de los resultados, la tipificación de los delitos informáticos.

Por todo lo expuesto, dejamos la idea de la necesidad de una reformulación o reorganización normativa, que tenga claridad sobre los bienes jurídicos afectados y una mejor regulación de las figuras de estudio, en el marco de una armonía legislativa que permita a futuro, forzar mejores lazos y agilizar la cooperación internacional.

8.2. Hipótesis 2: ¿Están adecuadamente reguladas las medidas o técnicas especiales de investigación?

Que, la segunda de las hipótesis planteada en nuestra tesis, postulaba que "*A nivel de normativa procesal penal, Argentina, Brasil, Colombia, México no han adecuado sus ordenamientos jurídicos para regular las medidas o técnicas especiales de investigación sugeridas por el Convenio de Budapest (art. 16 a 21) y el Proyecto de la Convención Internacional Integral sobre la Lucha contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos (art. 25 a 30). España es el único país de los incluídos en el estudio que se encontraría en cumplimiento".*

Que, consideramos apropiado que para dar una adecuada respuesta a la hipótesis sin caer en generalizaciones, es preciso que realicemos diferencias sobre los resultados en cada país.

Que, de acuerdo a la Tabla Nº 37a de las 5 jurisdicciones analizadas en Argentina, el 40% de ellas (CABA y el Fuero Federal) presentan graves problemas de regulación en el aspecto procesal penal (inferiores al 33,33%), siendo contundente una respuesta acerca de la insuficiencia normativa encontrada.

Que, aunque los casos de Mendoza, Neuquén y Salta (representando el 60% restante del alcance en Argentina), encuentran altos índices de cumplimiento muy buenos, debemos tener en consideración que existen un resto de jurisdicciones vigentes en la actualidad (20 Provincias restantes) que han sido excluidas por considerar que tenían un nulo o casi nulo desarrollo en la materia de interés.

Como conclusión, consideramos que lo más honesto -sin dejar de celebrar los casos de Mendoza, Neuquén, y sobre todo, de Salta-, es concluir en para el caso de Argentina la hipótesis planteada ha sido confirmada, es decir, no se encuentra en condiciones de considerarse un país con normativa procesal penal adecuada, en relación al estándar propuesto por los instrumentos internacionales revisados.

Que, en relación al caso de Brasil (fuero federal), es posible considerar como falsa la hipótesis planteada, toda vez que de acuerdo a la Tabla Nº 38a, Brasil presenta regulación vigente y aplicable en un 83,33% (5 de 6) de las medidas sugeridas internacionalmente, con lo que consideramos que sí podría llegarse a considerar adecuada su normativa actual.

Que, tanto México como Colombia exhiben un nivel de cumplimiento del 66,67% sobre estas medidas de investigación, por lo que de acuerdo a nuestro criterio, en este caso más restrictivo entendiendo que se trata de medidas fundamentales, consideramos como insuficiente como para firmar un dictamen que afirme que la regulación de dichos países se encuentra en cumplimiento de estándares internacionales.

Por último, la parte final de la hipótesis se invertía para el caso de España, nuestra referencia europea, estableciendo a priori que su regulación sí se encontraba en cumplimiento de los requisitos internacionales en materia procesal penal. Aquí también debemos confirmar la precisión de esta hipótesis, toda vez que España (junto a la Provincia de Salta -Argentina-), ha liderado el estudio con un 100% de cumplimiento sobre las medidas

Con la intención de traer mayor claridad para la persona lectora sobre las respuestas a esta segunda hipótesis de trabajo, dejamos el siguiente cuadro

:

País	Hipótesis planteada	Conclusión alcanzada
Argentina	No se encuentra adecuado a los estándares internacionales en materia procesal penal	Confirmada. Argentina no posee a nivel general estándares de cumplimiento adecuado a nivel procesal penal
Brasil	No se encuentra adecuado a los estándares internacionales en materia procesal penal	No confirmada. Brasil sí posee a nivel general estándares de cumplimiento adecuado a nivel procesal penal
Colombia	No se encuentra adecuado a los estándares internacionales en materia procesal penal	Confirmada. Colombia no posee a nivel general estándares de cumplimiento adecuado a nivel procesal penal
México	No se encuentra adecuado a los estándares internacionales en materia procesal penal	Confirmada. México no posee a nivel general estándares de cumplimiento adecuado a nivel procesal penal
España	Sí se encuentra adecuado a los estándares internacionales en materia procesal penal	Confirmada. España sí posee a nivel general estándares de cumplimiento adecuado a nivel procesal penal

Tabla Nº 41: Cuadro de confirmación de Hipótesis de Trabajo Nº 2

8.3. Consideraciones adicionales

A continuación, realizaremos breves comentarios sobre algunos temas que se han ido abordando en distintos momentos a lo largo de este trabajo, y que nos gustaría que de alguna forma, puedan quedar por su importancia, cristalizados aquí como una suerte de consideraciones a tener en cuenta u aspectos de relevancia relacionados con los delitos informáticos y el cibercrimen.

8.3.1. La asimetría de poder respecto de la investigación

Otro aspecto que nos gustaría dejar al menos visibilizado, es el hecho que la investigación de delitos informáticos presenta un desafío significativo para la defensa penal debido a la desigualdad de armas que existe frente a la fiscalía.

Esta disparidad se manifiesta en la falta de acceso a recursos y medidas investigativas por parte de la defensa, en contraste con los -en algunos casos amplios- recursos disponibles para las autoridades de persecución penal. La complejidad técnica y la rapidez con la que evolucionan las tecnologías hacen que sea aún más difícil para los abogados defensores mantenerse al día y proporcionar una representación efectiva para sus clientes en casos de delitos informáticos, que a diferencia de los funcionarios públicos, deben actualizarse de forma independiente.

En segundo lugar, esta desigualdad plantea serias preocupaciones en términos de equidad procesal y derechos fundamentales. La falta de acceso a recursos adecuados para la investigación por parte de la defensa puede resultar en una representación deficiente y en última instancia, esto implicar una vulneración del derecho a un juicio justo. Además, la asimetría en el acceso a la información y a los expertos técnicos puede conducir a sesgos -o en algunos casos errores- judiciales que terminan haciendo que su trabajo sea aún más complejo.

Adicionalmente, no podemos dejar de señalar que los costo de los operaciones de prácticas informático-forenses en el ámbito privado, son muy costosas, haciendo que una defensa igualitaria (accediendo a pericias informáticas) quede sólo reservado para los casos donde se cuenta con una billetera lo suficientemente importante para contratar a personas expertas en la materia.

En este sentido, consideramos importante que se tomen medidas para abordar esta desigualdad y garantizar que la defensa penal tenga acceso equitativo a los recursos necesarios para investigar y presentar sus casos de manera efectiva. Esto podría incluir la provisión de fondos públicos para la contratación de expertos técnicos y la implementación de políticas que promuevan la transparencia y el intercambio equitativo de información entre las partes en el proceso penal. Solo

mediante un enfoque equilibrado y justo se puede garantizar que los derechos de los acusados en casos de delitos informáticos sean protegidos de manera adecuada.

8.3.2. Identificar la investigación no convencional o compleja

El cibercrimen es a todas luces un delito no convencional, que para peor, se va actualizando y modificando en su modus operandi constantemente, obligando a las personas encargadas de su persecución, a capacitarse y a ser creativos a la hora de llevar adelante investigaciones que tengan alguna pretensión de eficacia.

En nuestra experiencia en la realización de capacitaciones a distintas fuerzas de seguridad en Argentina, observamos que suelen tener un pensamiento lineal (típico de las investigaciones convencionales) en el sentido que las investigaciones hacen uso de medidas de investigación, que a posteriori (en el caso que tengamos éxito en la búsqueda) nos brindará como resultado y consecuencia, datos (evidencia digital) que nos permitiría encontrar al delincuente y avanzar hacia su condena.

Sin embargo, entendemos que esa lectura unidireccional hacia la obtención de la evidencia digital, no suele dar buenas resultados o al menos no tan regularmente, por lo que rápidamente suele caerse en una frustración al momento de abordar la investigación de muchos de los delitos informáticos de la actualidad (sobre todo, si son parte de una banda de cibercriminales).

Es decir, debemos aprender a pensar que por un lado, podemos contar con evidencia digital desde un principio, sin siquiera haber ordenado una sola medida de investigación, por ejemplo, en los casos donde la víctima se acerca a la fiscalía y aporta evidencia digital que tiene en sus dispositivos electrónicos, o bien, la evidencia digital que será el eje de nuestra acusación, será posible conseguirla luego de un importante recorrido donde participará otra evidencia digital (en diferentes ciclos).

A nuestro criterio, esta situación trae como consecuencia los actuales problemas en materia de análisis de información y sus correspondientes dictámenes periciales, donde al momento de solicitar la extracción, los pedidos son tan amplios y difusos, que culminan en la realización de una extracción forense (física o lógica) de la totalidad de los datos del teléfono móvil, enviando la totalidad de dichos datos a la fiscalía para su revisión (evitando así la realización de los dictámenes forenses que deberían realizarse desde el laboratorio forense).

Si bien entendemos que en muchos casos esta situación puede tener como raíz la falta de recursos (falta de personal capacitado, falta de capacidad operativa en los laboratorios forenses, etc.), también es posible que otra de las razones sea que al momento de realizar dicha extracción forense, la fiscalía no tenga certeza acerca de qué datos podrían ser útiles para continuar con otras puntas de investigación.

Es decir, si desde el punto de vista lineal o unidireccional se intenta realizar preguntas concretas relacionadas a probar la culpabilidad de la persona investigada podría tener como resultado un dictamen negativo a los intereses de la fiscalía, sin embargo, si se aborda dicha información desde el punto de vista circular o complejo, quizás parte de esa información pueda llevar a otros rastros que hacen a la imagen más “grande” de la organización criminal.

8.3.3. La necesidad de una buena técnica legislativa

Aprovechamos la introducción de este ejemplo para sumar dentro de nuestras conclusiones finales, la importancia de la técnica legislativa. Si bien somos conscientes que no estamos descubriendo nada nuevo y que hay cientos de autores que han desarrollado este concepto extensamente, si nos parece oportuno destacar cómo, en una investigación que lo que busca es determinar la existencia de determinado tipo de regulación predeterminada por estándares internacionales, la técnica legislativa de los países se vuelve trascendental, toda vez que en muchos casos, aún teniendo Códigos Procesales Penales desactualizados, se han podido

encontrar figuras al menos que sean parcialmente aplicables, gracias al buen trabajo realizado en su momento.

Conectándo este concepto con todo lo desarrollado sobre los principios, entendemos que la ambiguedad o inexactitud en las normas procesales también provoca, en forma independiente, una violación al principio de *nulla coactio sine lege*de (y por lo tanto, en el fondo, una afectación al principio de *Nullum crimen, nulla poena sine praevia lege)*. De la misma manera que violamos la *nulla coactio* si aplicamos una medida de coerción que no se encuentra prevista normativamente, también la violamos si aplicamos conceptos o nos extendemos en demasía en la utilización de ciertos institutos, que deben -por la gravedad de su afectación- ser siempre de interpretación restrictiva.

Por otro lado, no encontramos mejor lugar para hacer mención a que la regulación de las medidas o técnicas especiales de investigación, deberían ser precisas en cuanto a los objetivos, límites, alcances, pero siempre manteniendo una neutralidad tecnológica. Es decir, que las normativas no deberían ahondar en propuestas o especificaciones técnicas concretas, toda vez que el rápido avance de la tecnología podría generar la obsolescencia de esa técnica, limitando el verdadero espíritu de esa norma.

8.3.4. El cibercrimen con perspectiva: un problema multifactorial

Que, insistiremos en la comprensión sobre la complejidad que representa el cibercrimen a nivel mundial, que más allá de contar con un plexo normativo adecuado, será siempre necesario contar con recursos humanos capacitados (y actualizados en la materia), así como recursos técnicos que permitan su adecuado desempeño.

A ello, es imprescindible sumar la importancia de contar con una fiscalía y un poder judicial también a la altura de las circunstancias, que tenga los conocimientos necesarios para agilizar el avance de las investigaciones. Sumado a esos

conocimientos, que se tenga (en ambos casos) la decisión política de darle a los ciberdelitos la importancia que merecen en su persecución.

También es necesario contar con un sector privado que se encuentre comprometido con la cooperación con la justicia, que también facilite el acceso (siempre con los requisitos adecuados por supuesto) a los datos que sean considerados de interés para las investigaciones en curso. Un sector privado desinteresado en la justicia, que no responda adecuadamente los pedidos de información, o que responda sosteniendo que no posee información que en realidad técnicamente si posee, pero que no quiere realizar el "gasto" que implica su búsqueda y entrega, pueden ser la ruina para toda una investigación.

Por ello volvemos a insistir. La existencia de un plexo normativo (a nivel material y procesal) es necesario, pero no es suficiente para garantizar una investigación adecuada de los delitos informáticos.

8.3.5. El conocimiento como co-construcción

Reconocemos que la temática elegida ha implicado un enorme desafío dogmático y académico para intentar ser lo más integral posible, sin salirnos del marco teórico y los objetivos inicialmente planteados.

Que, a lo largo de todo el trabajo, hemos ido dejando pequeños mojones o señales, destacando temas que, a nuestro criterio y juicio, son merecedores de un mayor nivel de profundización y abordaje, que por cuestiones de limitaciones de objeto y alcance, ha sido imposible de lograr en esta tesis por este autor.

Tenemos la esperanza que con el trabajo realizado, haber logrado generar un pequeño pero sostenible avance en la materia, tanto desde el punto de vista teórico normativo (generación del mapa de derecho comparado), así como en el aspecto de campo, a través de la propuesta final que dejamos a continuación en el capítulo.

Un avance que esperamos que futuros investigadores e investigadoras con interés en la temática puedan continuar desarrollando en pos de co-construir mayor nivel de conocimiento que nos permita, en definitiva, llevar adelante un combate eficaz contra la ciberdelincuencia.

8.4. La relación entre las hipótesis y la tesis

La validación de nuestra primera hipótesis, confirma que la adecuada tipificación de los delitos informáticos no resuelve el problema del cibercrimen. Entendemos que incluso la expansión penal de los delitos informáticos tipificados genera dentro del sistema penal, la aparición de nuevas denuncias (de los nuevos delitos tipificados) que, de acuerdo a los estudios repasados, en la mayoría de las Fiscalías -siempre hay excepciones- se observan importantes problemas de eficacia al momento de su investigación.

Hemos dejado claro a lo largo de este trabajo nuestra postura acerca que si bien la regulación de normativa penal material es fundamental y necesaria para mejorar la eficacia en la identificación, persecución y sanción de los ciberdelitos, no es suficiente. El problema es complejo, multifactorial.

Así fue como se incorporó la necesidad de sumar al estudio el aspecto procesal penal, entendiendo que era la nueva deuda existente en la materia, atento a que, tal como se confirmó a través de nuestra segunda hipótesis de trabajo, en países como Argentina, Brasil, Colombia y México, la adopción de normativa procesal penal ha sido desigual e insuficiente.

Entre las consecuencias de la ausencia de una normativa procesal penal específica podemos observar que por un lado deja a las autoridades nacionales en una posición de desventaja en materia de investigación frente a la sofisticación creciente de los delitos cibernéticos. Por otro lado, y tal como hemos visto en el Capítulo V, genera una desprotección e inseguridad jurídica que posibilita graves afectaciones a los derechos y libertades individuales de las personas.

Destacamos entonces la peligrosidad de permanecer en este estado de ausencia de normativa procesal penal, permite perpetuar un sistema que para continuar su funcionamiento, termina forzando de manera abusiva al principio de la "libertad probatoria" con la finalidad de justificar la incorporación de elementos de evidencia digital, sin que los mismos sean contrastados por controles y principios en resguardo de los derechos del sujeto investigado.

Reafirmamos nuestra convicción en que, la mejor forma de brindar garantías para la protección de los derechos y garantías de todas las personas, facilitar el trabajo tanto de la Fiscalía como del poder jurisdiccional, así como dotar de igualdad de armas a la defensa penal, es a través de una regulación adecuada y minuciosa de todas las medidas o técnicas especiales de investigación.

Sin embargo, la validación de la segunda hipótesis nos ha demostrado que aún queda un importante camino a recorrer para alcanzar esa situación ideal. En este contexto, nace la propuesta planteada como tesis de este trabajo, de desarrollar una **"Guía de Buenas Prácticas sobre medidas o técnicas especiales de investigación para el cibercrimen"**, que surge como una solución práctica a la laguna normativa existente. Esta guía tendría varios objetivos clave:

1. **Estandarización y Consenso Internacional**: Proporcionar una referencia común que facilite la armonización de las prácticas investigativas a nivel internacional. Aunque no vinculante, la guía podría servir como un marco de referencia que promueva la adopción de estándares mínimos en la investigación de delitos cibernéticos.
2. **Orientación y Capacitación**: Ofrecer a las autoridades nacionales y regionales un recurso valioso para el desarrollo de capacidades en la investigación del cibercrimen. La guía incluiría ejemplos de mejores prácticas, recomendaciones sobre la implementación de tecnologías de investigación, y pautas para la cooperación internacional.
3. **Protección de Derechos Fundamentales**: Uno de los principales desafíos en la lucha contra el cibercrimen es equilibrar la necesidad de medidas efectivas de investigación con la protección de los derechos fundamentales de los individuos. La guía abordaría este equilibrio, proporcionando recomendaciones claras sobre cómo minimizar la intrusión en la privacidad y otros derechos humanos durante las investigaciones.
4. **Flexibilidad y Adaptabilidad**: La naturaleza no vinculante de la guía permitiría a los diferentes países adaptarla a sus contextos legales y operativos específicos. Esto es crucial, dado que cada jurisdicción tiene sus propias particularidades legales y culturales que deben ser respetadas.

En resumen, la tesis viene a intentar una propuesta que permita mejorar el estado del arte en la materia, donde ha quedado demostrada la necesidad de un marco normativo robusto y estandarizado para la investigación del cibercrimen.

Por todo lo expuesto, entendemos que nuestra propuesta de guía no sólo proporciona orientación y estandarización sobre la normativa procesal penal tendiente a la incorporación de evidencia digital, sino que también contribuiría a la protección de los derechos fundamentales y a la mejora de la cooperación internacional en la lucha contra el cibercrimen.

Capítulo IX: Propuesta Final - Guía de Buenas Prácticas para la solicitud de Medidas o Técnicas Especiales de Investigación para casos de Cibercrimen

1.0. Introducción

La frase que acompaña el comienzo de esta tesis doctoral reza: "El pesimista se queja del viento; el optimista espera que cambie y el realista ajusta las velas" (George Ward).

Entendemos que luego de todo el estudio realizado, ser pesimista sería concluir con algún tipo de reproche o queja sobre la inactividad de los legisladores, que luego de tantos años aún no se han preocupado en adaptar su respectivo código procesal penal a fin de poder reparar una situación que, como hemos visto, desde el punto de vista estrictamente jurídico es muy difícil de defender.

Ser optimista, sería creer que esta situación podría ser solucionada en el corto o mediano plazo, esperando y confiando en que algún sector político de turno tome cartas en el asunto, asignando el proyecto a alguna comisión encargada de elaborar el proyecto, o esperar que algún legislador lo haga aisladamente.

Preferimos ser realistas, preferimos que hasta tanto cambie el viento y la normativa procesal penal en deuda sea efectivamente sancionada, podemos hacer algo al respecto, ajustar las velas proponiendo una norma alternativa, que dicho sea de paso, en el marco del extenso estudio realizado, no se ha encontrado nada similar al respecto.

Proponemos como entrega final, la generación de una “Guía de Buenas Prácticas sobre medidas o técnicas especiales de investigación para el cibercrimen”, que permita a todas aquellas jurisdicciones que aún no tienen normativa al respecto, poder tener un norte hacia donde caminar.

La guía pretende brindar un abanico de herramientas de investigación, indicando de acuerdo a los estándares internacionales que hemos observado, los límites y requerimientos recomendados, que claro está, no son obligatorios ni vinculantes, pero nuestro deseo es que sean útiles como referencia.

Referencia que podrá ser tomada tanto por los Ministerios Públicos Fiscales al momento de solicitar esas medidas de investigación. Referencias que podrán ser tomadas por el respectivo juez o jueza que tenga que autorizar o limitar las medidas solicitadas. Referencias que también podrán ser consideradas por la defensa penal, al momento de cuestionar arbitrariedades o abusos por parte de los funcionarios encargados de llevar adelante la investigación respectiva.

Teniendo claro que la publicación de la propuesta que forma parte del último capítulo de esta tesis se trata de una versión preliminar del documento, sin pretensiones de exactitud y completitud y que, en el caso que el mismo sea considerado de utilidad para su difusión abierta y pública, podrá con el paso del tiempo ir siendo parte de un proyecto más importante.

Sin más que agregar, y quedando siempre con la esperanza que nuestro aporte pueda sumar un granito de arena que nos permita, en definitiva, llevar adelante un combate eficaz contra la ciberdelincuencia.

2.0. Aspectos Generales

2.1. Alcance

La presente propuesta de la “Guía de Buenas Prácticas para la solicitud de Medidas o Técnicas Especiales de Investigación para casos de Cibercrimen” tiene como principales públicos objetivo a aquellas personas que desarrollen sus

actividades en el Ministerio Público Fiscal o en Fuerzas de Seguridad, e incluso, de Jueces o Juezas de Instrucción, dependiendo del país y de la forma de organización de la justicia (sistema acusatorio o inquisitivo).

2.2. Misión

La misión del proyecto es proponer una Guía que pueda ser tenida en consideración a nivel internacional (inicialmente Argentina y con pretensión de que sea útil también en Latinoamérica) como una referencia para todas aquellas jurisdicciones que de momento, no poseen una adecuada regulación en el ámbito procesal penal relacionada a medidas o técnicas especiales de investigación sobre evidencia digital. Con ese objeto, hemos bautizado a la propuesta como "Guía de Buenas Prácticas para la solicitud de Medidas o Técnicas Especiales de Investigación para casos de Cibercrimen".

Es decir, tendría como misión última aportar conocimiento tendiente a la obtención de información y elementos de convicción para descubrir o identificar a las personas involucradas en la comisión del delito informático, aportar pruebas al proceso sobre el delito investigado y, en su caso, prestar auxilio a autoridades extranjeras para estos mismos fines, teniendo siempre en cuenta la debida garantía de los derechos humanos y las libertades de las personas.

2.3. Visión

Este proyecto nace como corolario final de una tesis de doctorado dedicada a estudiar el estado actual de la problemática del cibercrimen, y donde hemos detectado que aún gran parte de las jurisdicciones estudiadas, tienen una deuda en relación a la regulación de las medidas y técnicas especiales de investigación para el cibercrimen.

De esta forma, el proyecto busca concientizar sobre dicha necesidad, poniendo de manifiesto que esta Guía de Buenas Prácticas sólo intenta mejorar o suplir la inexistencia normativa en la materia, en un contexto de una multiplicidad de

investigaciones formales que continúan realizándose y de medidas que se solicitan y aprueban diariamente, muchas veces, sin tener en cuenta el respeto por los derechos y garantías de las personas.

A partir de la necesidad de dar a conocer el problema de la falta o inadecuada normativa en materia procesal penal que permita mayor seguridad jurídica al momento de solicitar medidas de investigación para los delitos informáticos, este proyecto pretende por un lado tener una función académica y formativa sobre qué significa cada medida de investigación, indicando los límites que deberían considerarse y divulgando una cultura de generar pedidos de autorización con mayor sustento en los fundamentos y mayor respeto hacia los principios normativos.

Por otro lado, se plantea una función más concreta, que es que a partir de la utilización de un sistema informático que hemos desarrollado, permitir que el usuario (personal de la fiscalía o fuerza de seguridad involucrada en la investigación) pueda contar con un recurso práctico que permita, a partir de responder ciertas datos concretos que deberían -a nuestro criterio- formar parte de la solicitud de la medida, generar de forma automatizada un modelo de escrito, que pueda servir como referencia para realizar los pedidos en su propia jurisdicción.

2.4. Objetivos generales

- Visibilizar y difundir información relevante para estudiar, investigar e incidir en la problemática de la ausencia o deficiencia de la normativa procesal penal relacionada a la investigación de los delitos informáticos.
- Proponer una alternativa que permita combatir temporal o parcialmente el problema de la ausencia o deficiencia de normativa procesal penal en la generación de medidas o técnicas especiales de investigación para el cibercrimen en los países de América Latina.

2.5. Objetivos específicos

- Aportar conocimiento académico sobre las distintas medidas o técnicas de investigación posibles.
- Fomentar la existencia de límites y requisitos que deben ser tenidos en cuenta de acuerdo al tipo de medida o técnica de investigación seleccionada.
- Aportar una herramienta útil para mejorar la redacción y generación de solicitudes de medidas o técnicas de investigación.
- Generar informes y estadísticas propias sobre las medidas o técnicas de investigación más utilizadas por parte de las Unidades Fiscales o Fuerzas de Seguridad.

3.0. Metodología y Desarrollo del Sistema

El Proyecto será llevado a cabo a través de un sitio web, aunque al momento de escribir estas líneas, aún está por definirse si se encontrará dentro del dominio ya existente del Observatorio de Delitos Informáticos de Latinoamérica (ODILA) - www.odila.org o será un proyecto con un dominio propio.

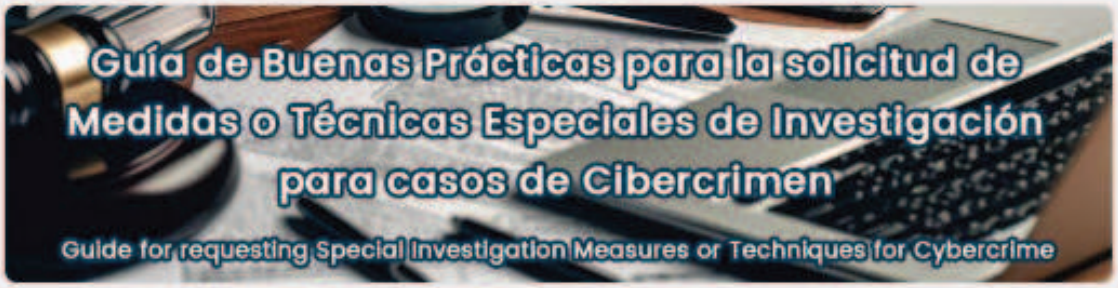
En el sitio web, el usuario podrá encontrar información sobre el proyecto, y un acceso directo para descargarse la última versión de la "Guía de Buenas Prácticas para la solicitud de Medidas o Técnicas Especiales de Investigación para casos de Cibercrimen" en formato pdf.

En el mismo sitio web, el usuario podrá encontrar el enlace directo para acceder y hacer uso del sistema online de generación de solicitudes de medidas de investigación.

A continuación, desarrollaremos en pasos y etapas el funcionamiento del circuito completo del sistema generado:

3.1. Ingreso al sistema

- Al ingresar al sistema, el usuario será recibido con un mensaje de bienvenida, con un aviso legal de tres cláusulas breves, que buscará evitar malas interpretaciones o inconvenientes en relación a los objetivos y pretensiones del proyecto, cuyo detalle podrá observarse entre las aclaraciones importantes que se realizan en la sección 4 de este capítulo.
- Al finalizar el aviso, se advierte al Usuario presionar en el botón "Siguiente" implica una manifestación de voluntad en sentido positivo, y se considera que estará aceptando las condiciones para acceder al uso del sistema. En caso de no aceptar dicho aviso legal, estará imposibilitado de acceder al sistema.



Guia de Buenas Prácticas para la solicitud de Medidas o Técnicas Especiales de Investigación para casos de Cibercrimen

Versión preliminar 1.0 - **Autor: Abog. Marcelo Temperini** - mtemperini@asegurarte.com.ar

Para acceder a la Guía Completa acceder aquí: **link**

mtemperini@asegurarte.com.ar Cambiar de cuenta

No compartido

Aviso Legal

- *El presente sistema o los escritos generados por el mismo, no deben ser considerados bajo ningún punto de vista como un asesoramiento profesional para el usuario, pensado para el uso interno de Ministerios Públicos Fiscales, así como Fuerzas de Seguridad vinculadas a la investigación del ciberdelito.*
- *El sistema no garantiza la exactitud de los resultados en relación a sobre si la medida o técnica especial de investigación solicitada puede o no pedirse en la jurisdicción a la que pertenece el usuario, ni si su sistema normativo permite o no la ejecución de la misma.*
- *El objetivo de la "Guía de Buenas Prácticas para la solicitud de Medidas o Técnicas Especiales de Investigación para casos de Cibercrimen" es fomentar la realización de pedidos de medidas de investigación, que tengan un mayor nivel de respeto y compromiso por los derechos fundamentales, estimulando la práctica de fundamentar las medidas de acuerdo a su necesidad, razonabilidad y proporcionalidad.*

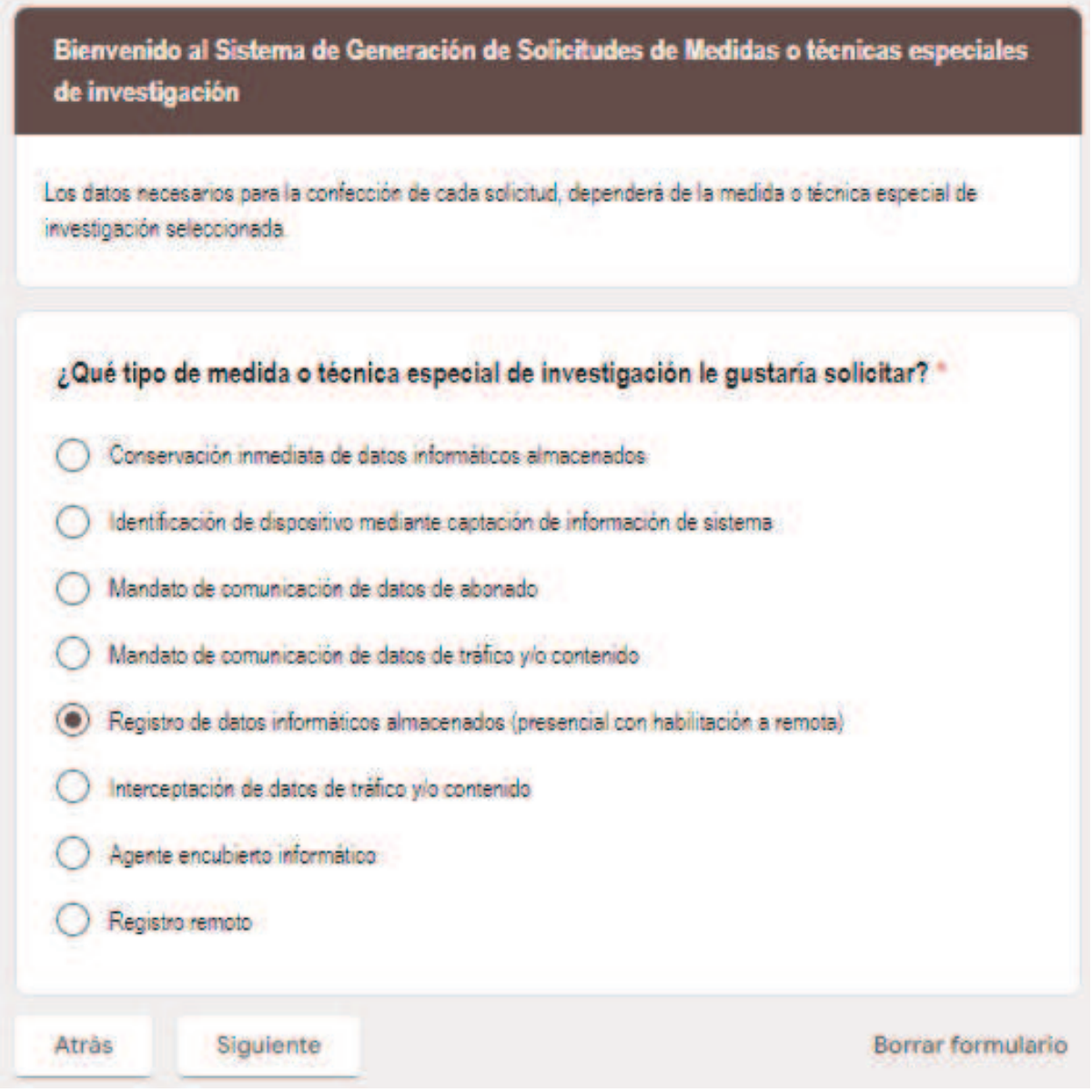
Aceptación de Términos Legales

Entiendo que al presionar en "Siguiente", estaré aceptando las condiciones para acceder al uso del sistema de generación de pedidos de medidas o técnicas especiales de investigación para Cibercrimen

Siguiente Borrar formulario

3.2. Selección de medidas o técnica especial de investigación

- En caso de aceptar y avanzar, la siguiente pantalla exhibirá información de las distintas medidas o técnicas de investigación disponibles en el sistema. En la versión preliminar 1.0 del sistema, se ha decidido comenzar con las siguientes ocho (8) medidas o técnicas de investigación.

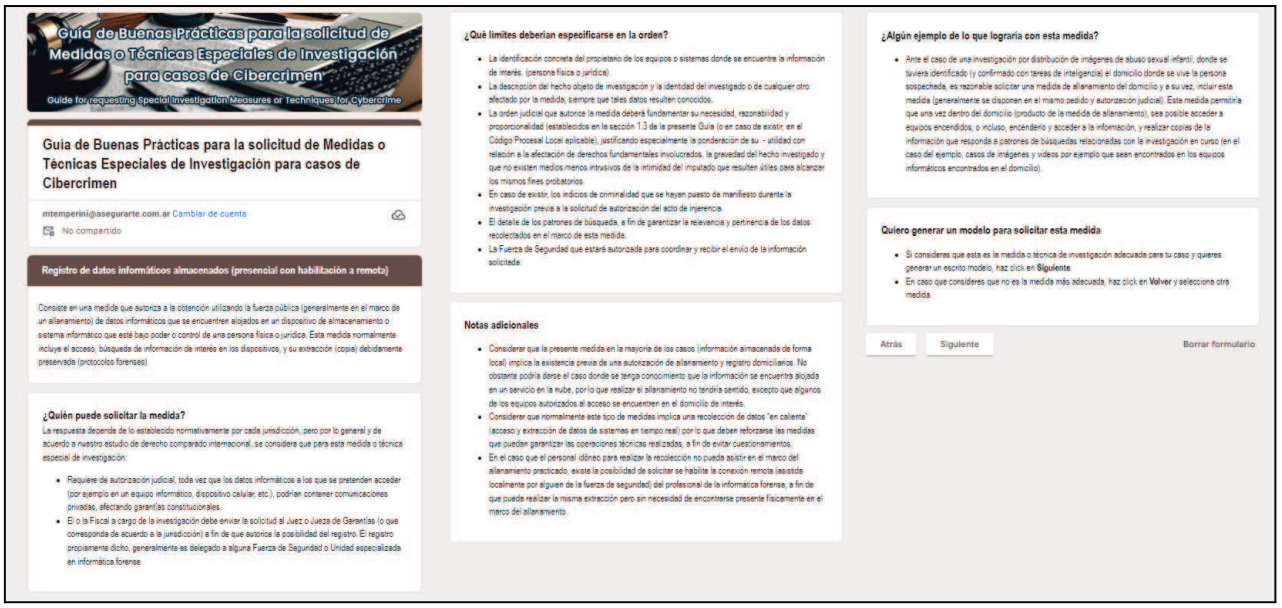


Las medidas o técnicas especiales cargadas en la versión preliminar son:

- Conservación inmediata de datos informáticos almacenados

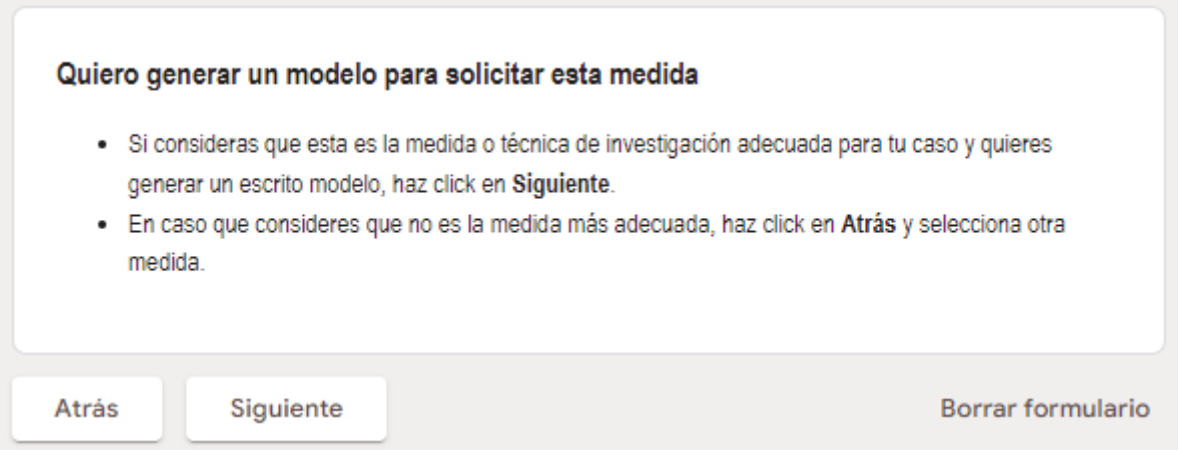
- Identificación de dispositivo mediante captación de información de sistema
- Mandato de comunicación de datos de abonado
- Mandato de comunicación de datos de tráfico y/o contenido
- Registro de datos informáticos almacenados (presencial con habilitación a remota)
- Interceptación de datos de tráfico y/o contenido
- Agente encubierto informático
- Registro remoto

- A partir de la medida o técnica de investigación seleccionada por el usuario, el sistema dará acceso a una nueva pantalla donde se exhibirá información que dará respuesta a los siguientes interrogantes:
  - ¿En qué consiste la medida?
  - ¿Quién puede solicitarla?
  - ¿Qué límites deberían especificarse en la orden?
  - Notas adicionales
  - ¿Algún ejemplo concreto del uso de esta medida o técnica especial de investigación?



Pantalla recortada a modo de ejemplo, ya que el desarrollo de todos interrogantes, implicaría realizar varias capturas para exhibir la totalidad de la información brindada.

- En el caso que el usuario considere que dicha medida o técnica de investigación es la más adecuada para su caso, el usuario deberá seleccionar la opción “Quiero generar un modelo para solicitar esta medida” y de esa forma podrá avanzar hacia la segunda etapa de la herramienta. En caso que la medida no sea la más adecuada, podrá presionar en el botón “Atrás” y volver al menú de selección de medidas.



3.3. Recolección de datos sobre la medida seleccionada

- En la nueva etapa y de acuerdo al tipo de medida o técnica de investigación seleccionada, el sistema realizará una serie de preguntas al usuario, que serán necesarias para poder dar lugar a que el sistema pueda generar el escrito modelo final para enviarle al usuario. A continuación realizaremos un detalle por las preguntas o datos solicitados por cada medida o técnica especial de investigación seleccionada:
    - **Conservación inmediata de datos informáticos almacenados**
        i. A1- Nombre del Proveedor de Servicios (ISP o CSP):
        ii. A2- Dirección del Proveedor de Servicios (ISP o CSP)
        iii. A3- Nombre de usuario del perfil que me interesa preservar:
        iv. A4- User ID del perfil que me interesa preservar:
        v. A5- Url del perfil que me interesa preservar:
        vi. A6- Plazo de la conservación solicitada:
        vii. A7- Solicitar confidencialidad de la medida:

viii. A8- Nombre de la fuerza de seguridad o fiscalía autorizada a realizar el diligenciamiento de la medida:

ix. A9- Mail de contacto para indicar en el escrito para que el proveedor de servicios pueda comunicarse:

- **Identificación de dispositivo mediante captación de información de sistema**
  i. B1- Nombre de la unidad o división de la Fuerza de Seguridad que ejecutará la medida:
  ii. B2- Dirección de la unidad o división de la Fuerza de Seguridad que ejecutará la medida:
  iii. B3- Datos del sistema / usuario / dispositivo con el que se desea interactuar para obtener información:
  iv. B4- Plazo autorizado para la ejecución:
  v. B5- Técnica particular que se utilizaría para la obtención de la información:
  vi. B6- Mail de contacto de la fuerza de seguridad que ejecutará la medida:
- **Mandato de comunicación de datos de abonado**
  i. C1- Nombre del Proveedor de Servicios (ISP o CSP)
  ii. C2- Dirección del Proveedor de Servicios (ISP o CSP)
  iii. C3- Fundamentos:
  iv. C4- Datos de la cuenta / usuario / IP de la que se solicita información:
  v. C5- Nombre de la unidad o división de la Fuerza de Seguridad que ejecutará la medida:
  vi. C6- Mail de contacto de la fuerza de seguridad que ejecutará la medida:
- **Mandato de comunicación de datos de tráfico y/o contenido**
  i. D1- Nombre del Proveedor de Servicios (ISP o CSP)
  ii. D2- Dirección del Proveedor de Servicios (ISP o CSP)
  iii. D3- Fundamentos:

iv. D4- Datos de la cuenta / usuario / IP de la que se solicita información:
v. D5- Nombre de la unidad o división de la Fuerza de Seguridad que ejecutará la medida:
vi. D6- Mail de contacto de la fuerza de seguridad que ejecutará la medida:

- **Registro de datos informáticos almacenados (presencial con habilitación a remota)**
  i. E1- Persona física o jurídica propietaria de los sistemas objeto de la medida:
  ii. E2- Domicilio donde se encuentran los equipos o sistemas informáticos objeto de la medida:
  iii. E3- Fundamentos:
  iv. E4- Palabras clave:
  v. E5- Nombre de la unidad o división de la Fuerza de Seguridad que ejecutará la medida:
- **Interceptación de datos de tráfico y/o contenido**
  i. F1- Nombre del Proveedor de Servicios (ISP o CSP)
  ii. F2- Dirección del Proveedor de Servicios (ISP o CSP)
  iii. F3- Persona o cuenta de interés para interceptar:
  iv. F4- Fundamentos:
  v. F5- Plazo de interceptación de datos:
  vi. F6- Nombre de la unidad o división de la Fuerza de Seguridad autorizada a diligenciar la medida:
  vii. F7- Mail autorizado de la unidad o división de la Fuerza de Seguridad:
- **Agente encubierto informático**
  i. H1- Cuenta o persona investigada:
  ii. H2- Fundamentos:
  iii. H3- Plazo de actuación del agente encubierto informático:
  iv. H4- Nombre de la unidad o división de la Fuerza de Seguridad autorizada a diligenciar la medida:

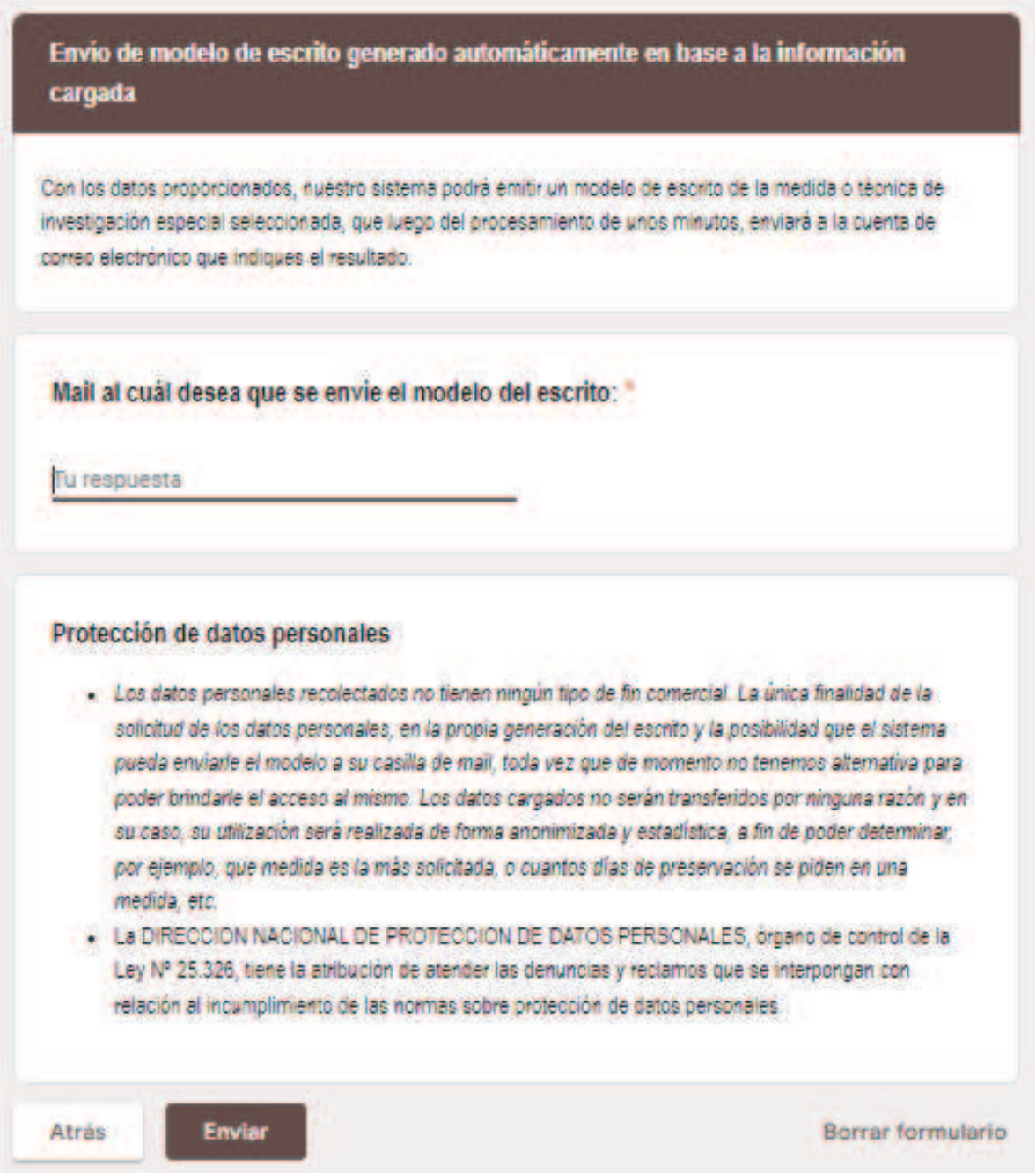
v. H5- Incluir en la solicitud la posibilidad de habilitar acciones especiales:

- **Registro remoto**
  i. J1- Persona o cuenta / sistema objeto de la medida:
  ii. J2- Datos técnicos del sistema objeto de la medida:
  iii. J3- Plazo de actuación del registro remoto:
  iv. J4- Software habilitado para uso:
  v. J5- Fundamentos:
  vi. J6- ¿Solicitar dejar puerta trasera abierta?
  vii. J7- Nombre de la unidad o división de la Fuerza de Seguridad autorizada a diligenciar la medida:

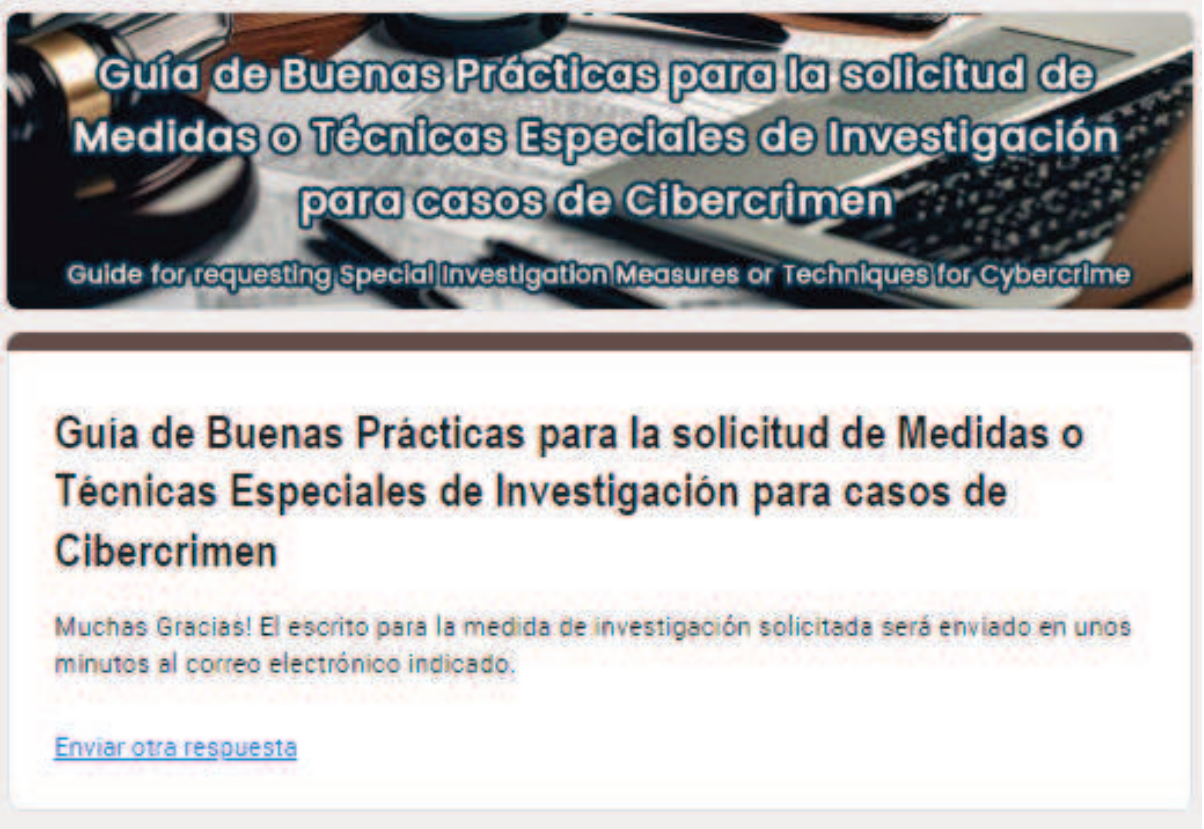
- Una vez que el usuario completó toda la información requerida de acuerdo a su elección, el sistema lo dejará avanzar hacia la última etapa. En caso de detectar que alguna pregunta no fue respondida, el sistema indicará dicha situación, obligando al usuario a completar dichos datos para poder continuar.

3.4. Indicación de mail para el envío del escrito

- Con todos los datos, el usuario avanzará hacia una nueva pantalla final del sistema, donde se informará que con los datos proporcionados el sistema emitirá un modelo de escrito de la medida o técnica de investigación especial seleccionada, que tras unos minutos de procesamiento, será enviado a la cuenta de correo electrónico que se deberá indicar en esa pantalla final. Es decir, aquí será el único momento donde el usuario deberá indicar un correo electrónico “real”, a fin de poder efectivamente recibir el escrito generado (ver mayor detalle de este punto en el punto 4.3. de la sección siguiente)
- Una vez cargado el correo electrónico donde se recibirá el escrito generado, el usuario deberá realizar el envío final de los datos del formulario, no sin antes exhibir una leyenda legal relacionada a la recolección de los datos personales (toda vez que la recolección de dicho correo electrónico, implica la construcción y procesamiento de una base de datos).



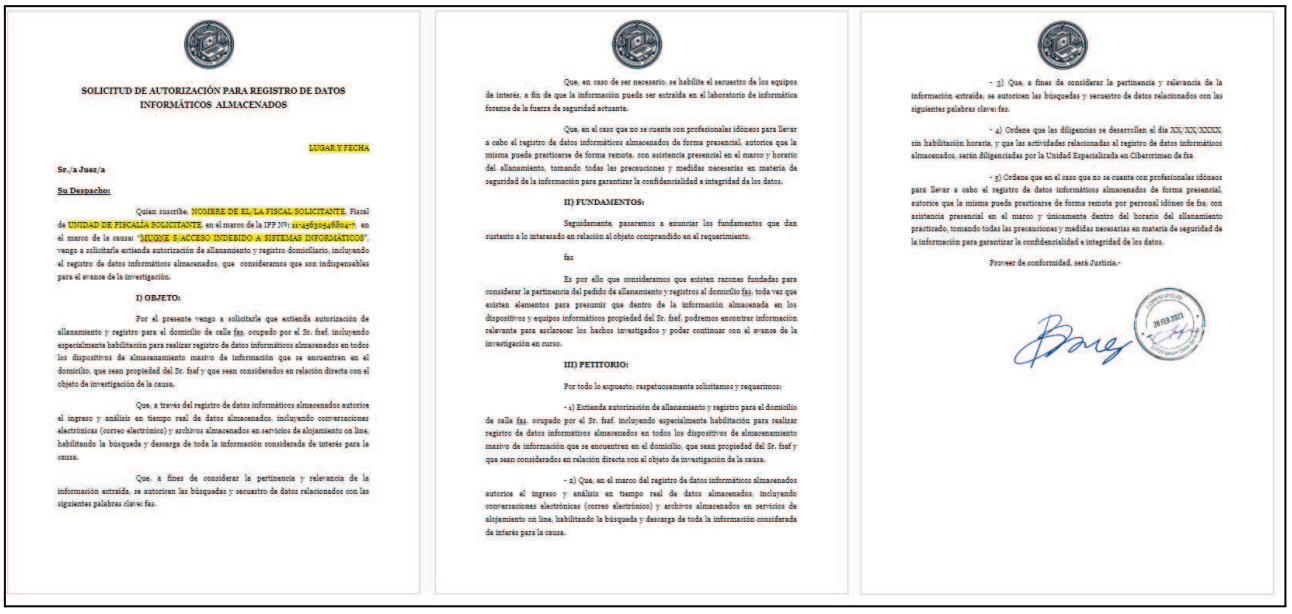
- Una vez enviados los datos, el usuario finaliza el proceso donde se le exhibe el siguiente mensaje: *"Muchas Gracias! El escrito para la medida de investigación solicitada será enviado en unos minutos al correo electrónico indicado."*



3.5. Envío de información a base de datos y procesamiento del sistema

- Paso siguiente, cuando el usuario presiona en el botón “Enviar” todos los datos del formulario son enviados a una base de datos, donde los mismos son organizados y segmentados a fin de que el sistema de generación automática de solicitudes de medidas, pueda consumir los datos desde allí.
    - De dicha base de datos, anualmente se proyecta realizar un informe estadístico que brinde transparencia, comunicando el nivel de uso semanal o mensual del sistema, brindando estadísticas sobre las medidas o técnicas más seleccionadas, entre otros datos de interés.
- Paso siguiente, si bien el sistema desarrollado se encuentra constantemente funcionando, el mismo se ha configurado para que se active cada vez que se agrega un nuevo registro (un pedido de escrito) dentro de la base de datos.

- Al detectarse el nuevo registro, el sistema consulta que tipo de medida o técnica especial de investigación se ha seleccionado y en base a dicho criterio, seleccionará una de las plantillas de escritos que ya previamente hemos generado y cargado dentro del sistema (la que corresponda con la medida seleccionada por el usuario).
- Una vez seleccionada la plantilla, el sistema se ha desarrollado accede a las respuestas brindadas por el usuario (ya cargadas y categorizadas en la base de datos) y las inyecta dentro del modelo de escrito seleccionado, a fin de que el mismo quede customizado o personalizado para el caso concreto de interés del usuario.
- Una vez generado el escrito con toda la información del usuario, el mismo es alojado dentro de una carpeta compartida en Google Drive preseleccionada.
- A continuación, compartimos una muestra en miniatura (por la extensión) de uno de los escritos generados automáticamente por el sistema.



SOLICITUD DE AUTORIZACIÓN PARA REGISTRO DE DATOS INFORMÁTICOS ALMACENADOS

LUGAR Y FECHA

Sr./a Juez/a

Su Despacho:

Quien suscribe, NOMBRE DE EL/LA FISCAL SOLICITANTE, Fiscal de UNIDAD DE FISCALÍA SOLICITANTE, en el marco de la IPP Nº: 21246950468049, en el marco de la causa: "MEDIDA S/ACCESO INDEBIDO A SISTEMAS INFORMÁTICOS", vengo a solicitarle sea autorización de allanamiento y registro domiciliario, incluyendo el registro de datos informáticos almacenados, que consideramos que son indispensables para el avance de la investigación.

I) OBJETO:

Por el presente vengo a solicitarle que sea autorización de allanamiento y registro para el domicilio de calle fas, ocupado por el Sr. fsaf, incluyendo especialmente habilitación para realizar registro de datos informáticos almacenados en todos los dispositivos de almacenamiento masivo de información que se encuentren en el domicilio, que sean propiedad del Sr. fsaf y que sean considerados en relación directa con el objeto de investigación de la causa.

Que, a través del registro de datos informáticos almacenados autorice el ingreso y análisis en tiempo real de datos almacenados, incluyendo conversaciones electrónicas (correo electrónico) y archivos almacenados en servicios de alojamiento on line, habilitando la búsqueda y descarga de toda la información considerada de interés para la causa.

Que, a fines de considerar la pertinencia y relevancia de la información extraída, se autoricen las búsquedas y secuestro de datos relacionados con las siguientes palabras clave: fas.

Que, en caso de ser necesario, se habilite el secuestro de los equipos de interés, a fin de que la información pueda ser extraída en el laboratorio de informática forense de la fuerza de seguridad actuante.

Que, en el caso que no se cuente con profesionales idóneos para llevar a cabo el registro de datos informáticos almacenados de forma presencial, autorice que la misma pueda practicarse de forma remota, con asistencia presencial en el marco y horario del allanamiento, tomando todas las precauciones y medidas necesarias en materia de seguridad de la información para garantizar la confidencialidad e integridad de los datos.

II) FUNDAMENTOS:

Seguidamente, pasaremos a enunciar los fundamentos que dan sustento a lo interesado en relación al objeto comprendido en el requerimiento.

fas

Es por ello que consideramos que existen razones fundadas para considerar la pertinencia del pedido de allanamiento y registros al domicilio fas, toda vez que existen elementos para presumir que dentro de la información almacenada en los dispositivos y equipos informáticos propiedad del Sr. fsaf, podremos encontrar información relevante para esclarecer los hechos investigados y poder continuar con el avance de la investigación en curso.

III) PETITORIO:

Por todo lo expuesto, respetuosamente solicitamos y requerimos:

- a) Extienda autorización de allanamiento y registro para el domicilio de calle fas, ocupado por el Sr. fsaf, incluyendo especialmente habilitación para realizar registro de datos informáticos almacenados en todos los dispositivos de almacenamiento masivo de información que se encuentren en el domicilio, que sean propiedad del Sr. fsaf y que sean considerados en relación directa con el objeto de investigación de la causa.

- b) Que, en el marco del registro de datos informáticos almacenados autorice el ingreso y análisis en tiempo real de datos almacenados, incluyendo conversaciones electrónicas (correo electrónico) y archivos almacenados en servicios de alojamiento on line, habilitando la búsqueda y descarga de toda la información considerada de interés para la causa.

- c) Que, a fines de considerar la pertinencia y relevancia de la información extraída, se autoricen las búsquedas y secuestro de datos relacionados con las siguientes palabras clave: fas.

- d) Ordene que las diligencias se desarrollen el día XX/XX/XXXX, sin habilitación horaria, y que las actividades relacionadas al registro de datos informáticos almacenados, serán diligenciadas por la Unidad Especializada en Cibercrimen de fas

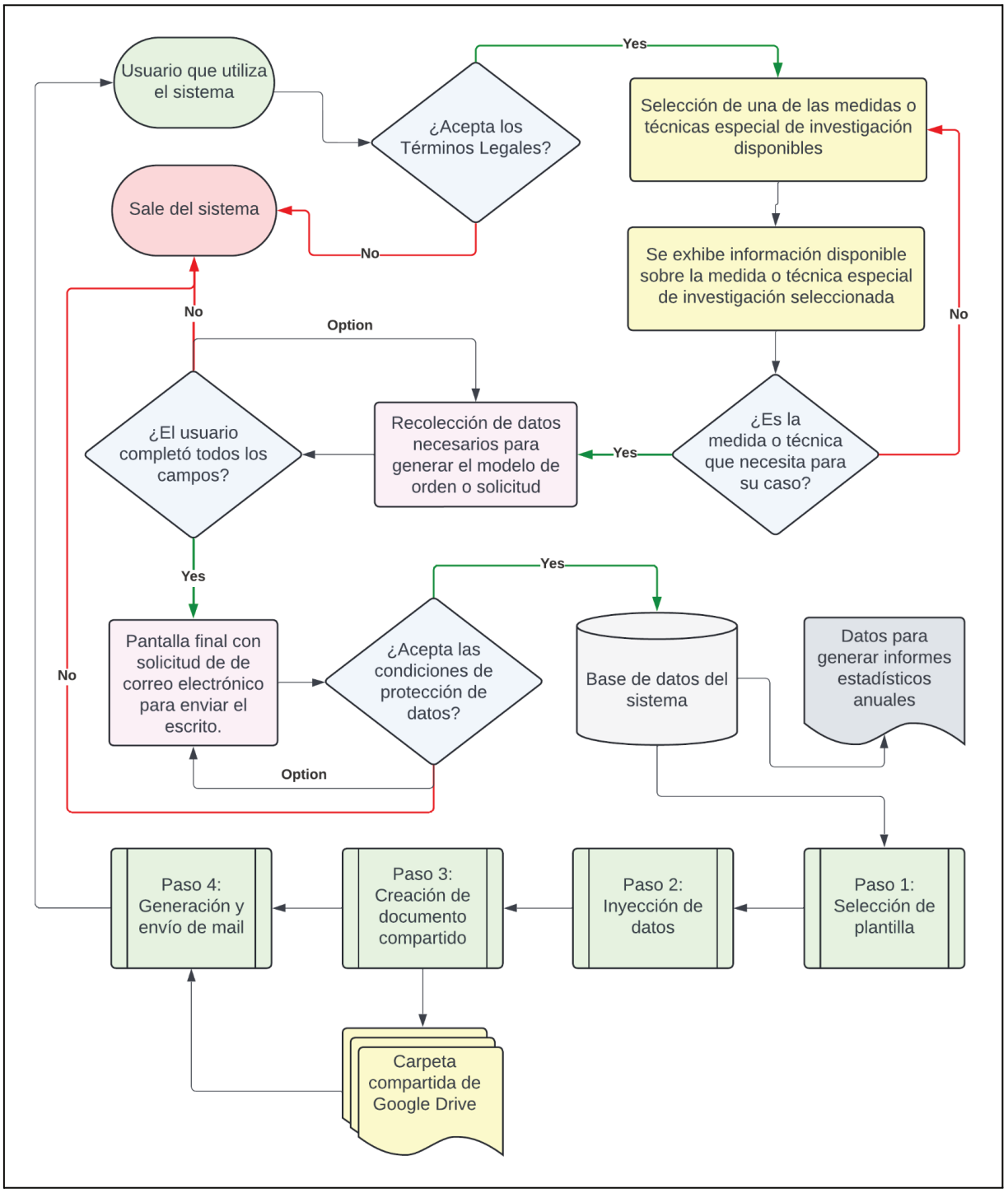
- e) Ordene que en el caso que no se cuente con profesionales idóneos para llevar a cabo el registro de datos informáticos almacenados de forma presencial, autorice que la misma pueda practicarse de forma remota por personal idóneo de fas, con asistencia presencial en el marco y únicamente dentro del horario del allanamiento practicado, tomando todas las precauciones y medidas necesarias en materia de seguridad de la información para garantizar la confidencialidad e integridad de los datos.

Proveer de conformidad, será Justicia.-

- El sistema genera un correo electrónico con un mensaje predeterminado (ver punto 4.3) incluyendo el enlace del documento compartido generado en el punto anterior, finalizando de esta forma con el circuito.

3.6. Diagrama de flujo del sistema generado

A continuación, compartimos un diagrama de flujo que intenta reflejar de forma gráfica los distintos pasos y etapas previamente desarrollados.



4.0. Aclaraciones importantes

4.1. Términos Legales

Como se ha advertido anteriormente, es de importancia hacer destacar (y que el usuario comprenda y acepte como se ha indicado en el primer paso del sistema) que el objetivo de la "Guía de Buenas Prácticas para la solicitud de Medidas o Técnicas Especiales de Investigación para casos de Cibercrimen" es fomentar la realización de pedidos de medidas de investigación, que tengan un mayor nivel de respeto y compromiso por los derechos fundamentales, estimulando la práctica de fundamentar las medidas de acuerdo a su necesidad, razonabilidad y proporcionalidad.

Por otro lado, destacamos que el sistema desarrollado o los escritos generados por el mismo, no deben ser considerados bajo ningún punto de vista como un asesoramiento profesional para el usuario. Debe comprenderse que el objeto del proyecto, es ser utilizado como una referencia y guía, pensado para el uso interno de Ministerios Públicos Fiscales, así como Fuerzas de Seguridad vinculadas a la investigación del ciberdelito.

Por último, afirmar que el sistema no garantiza que se encuentre libre de errores, ni la exactitud de los resultados en relación a sobre si la medida o técnica especial de investigación solicitada puede o no pedirse en la jurisdicción a la que pertenece el usuario, ni si su sistema normativo permite o no la ejecución de la misma, aspectos que deberán ser evaluados y dirimidos en cada caso particular.

4.2. Protección de datos personales

En relación a la protección de datos personales, como se ha destacado en el paso Nº 9 del sistema, el mismo advierte que para su funcionamiento, el mismo deberá procesar uno o más datos personales. Por dicho motivo, el sistema exhibe las siguientes cláusulas al usuario:

"Los datos personales recolectados no tienen ningún tipo de fin comercial. La única finalidad de la solicitud de los datos personales, en la propia generación del escrito y la posibilidad que el sistema pueda enviarle el modelo a su casilla de mail, toda vez que de momento no tenemos alternativa para poder brindarle el acceso al mismo. Los datos cargados no serán transferidos por ninguna razón y en su caso, su utilización será realizada de forma anonimizada y estadística, a fin de poder determinar, por ejemplo, qué medida es la más solicitada, o cuantos días de preservación se piden en una medida, etc.

La DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES, órgano de control de la Ley Nº 25.326, tiene la atribución de atender las denuncias y reclamos que se interpongan con relación al incumplimiento de las normas sobre protección de datos personales."

Con respecto al tema de la recolección de datos, se aclara que en dicho proceso es necesario que el usuario brinde un único dato personal "real": el correo electrónico, a fin de que el escrito generado por el sistema pueda ser enviado a dicha casilla.

Afirmamos que dicho dato debe ser real, porque es posible que entre las preguntas del escrito, se consulten otros datos personales, como por ejemplo una dirección IP, una cuenta de usuario o la cuenta de correo electrónico de la fuerza de seguridad que estará habilitada para que el proveedor de servicios envíe la información solicitada. En dicha información (la solicitada en relación al contenido de la medida solicitada), el usuario podrá cargar cualquier dato, sin necesidad que sea un correo real, toda vez que el mismo posteriormente podrá ser modificado en el escrito enviado (que es editable).

Por otro lado y a fines de preservar la privacidad de los usuarios y la confidencialidad de las causas investigadas con el mayor nivel posible, en los escritos hemos dejado que los datos referidos a la propia causa (Unidad Fiscal solicitante, Nº de causa, carátula de la causa, nombre del juez, nombre del o la fiscal que solicita, entre otros detalles) pintados de color amarillo, para que el usuario pueda reemplazarlos una vez que se descargue el escrito. A nuestro criterio, entendimos que si bien podríamos haber solicitado dicha información y generado los

escritos con toda esa información completa, dicha acción no era estrictamente necesaria y podría haber implicado que muchos usuarios no se animen o prefieran no experimentar el sistema por temor a revelar información confidencial de la causa en curso.

Entre las mejoras a realizarse a futuro esperamos que el escrito pueda ser generado y ofrecido sin necesidad de dejar ningún dato personal, a fin de preservar en la mayor medida posible, la privacidad del usuario.

4.3. Envío de correo electrónico al usuario

En el paso final del circuito (Paso Nº 14), cuando el sistema ha generado el escrito solicitado, este es enviado por correo electrónico al usuario, con el siguiente texto (aplicable para todas las medidas):

Estimad@, Le adjuntamos la versión del boceto de pedido o solicitud de medida de investigación. Tenga en consideración que por cuestiones de capacidad en nuestro sistema, el escrito estará disponible online sólo por 48 hs antes de ser eliminado, por lo que recomendamos que acceda y se descargue el mismo de forma local. Recuerde que el modelo es sólo con fines orientativos y académicos, por lo que recomendamos que si realmente quiere realizar uso formal en procesos judiciales del mismo, previamente revise y complete todos los datos que no han sido solicitados a fin de mantener en la mayor medida posible, la privacidad de los usuarios. Gracias por usar nuestro sistema. Por cualquier duda sobre el proyecto, puede contactarme al correo electrónico: mtemperini@asegurarte.com.ar

Consideramos de importancia, destacar el hecho que el correo electrónico enviado incluye de forma adjunta el link al escrito, que temporalmente queda guardado en una carpeta compartida en Google Drive.

Por tal motivo, y considerando que por lo preliminar del proyecto no se dispone de capacidad ilimitada para guardar los escritos por tiempo indeterminado, se ha considerado adecuado establecer como tiempo razonable, un plazo de 48 hs de compromiso por parte del proyecto, de guarda y disposición de dicho escrito, para

que posteriormente se tenga la libertad de poder ir eliminando los escritos generados de dicha carpeta.

Consideramos que no existe una razón particular para conservar los escritos generados por más tiempo, toda vez que en caso que el usuario requiera el mismo, podrá volver a utilizar el sistema y generar uno nuevo. Asimismo, consideramos que la eliminación cada cierto plazo de este tipo de información, podría contribuir a mantener de la mejor manera posible los estándares buscados sobre la privacidad.

5.0. Mejoras a futuro

5.1. Inclusión de más opciones de medidas o técnicas especiales de investigación

Como se ha mencionado anteriormente, la versión 1.0 de este proyecto ha comenzado con 8 (ocho) medidas o técnicas especiales de investigación, que a nuestro criterio y de acuerdo a nuestro estudio, consideramos que hoy serían el menú básico de herramientas con el que se debería contar para investigar los delitos informáticos.

Sin embargo, entendemos que existen diferentes modalidades de las propias medidas. Por ejemplo, en el caso de la medida de “Interceptación de datos de tráfico y/o contenido”, hemos trabajado un tipo de solicitud donde dicha interceptación es ejecutada técnicamente por un proveedor de servicios (por ejemplo Telecom). Sin embargo, nos queda pendiente realizar otra versión de la misma medida, donde la interceptación técnica sea realizada directamente por personal especializado de la fuerza de seguridad designada.

Por otro lado, a nuestro criterio también existe la posibilidad de combinar modalidades o habilitaciones dentro de las propias medidas o técnicas especiales de investigación. Por ejemplo, en el caso del “Registro de datos informáticos almacenados”, hemos optado por generar un escrito donde la habilitación o autorización sea para realizar el registro presencial pero con un agregado que

permitiría o habilitaría que las operaciones técnicas de extracción forense sean realizadas por el personal forense de forma remota, con asistencia técnica personal en el lugar de los hechos (allanamiento concretamente).

De esta forma, entendemos que incluso se pueden dar mayor nivel de combinaciones de las medidas. Por ejemplo, que este mismo registro de datos informáticos almacenados, se pueda solicitar con o sin "cláusula de acceso transfronterizo de datos", o bien, con o sin "cláusula de obligación de notificación de hallazgos casuales sobre evidencia digital". Claramente, este tipo de inclusión explícita sobre algunas situaciones sólo tendrían sentido en el caso que, la norma de fondo (procesal penal del lugar de la jurisdicción donde se intente utilizar este pedido) sea inexistente o menos rigurosa que lo que se establece en el pedido.

Entendemos que siempre y en todos los casos, la existencia (como se puede observar a lo largo del trabajo de la tesis) de algún tipo de normativa aplicable o parcialmente aplicable, será el piso normativo que bajo ningún aspecto podría -o muy excepcionalmente- podría contradecirse. Por eso, buscamos que el proyecto brinde propuestas de escritos que sean, en la medida de lo posible, lo más respetuosas de las libertades y garantías de las personas, que es en definitiva, parte de la misión a lograrse.

Realizado todo este desarrollo previo, y para cerrar este primer apartado de mejoras a futuro, dejamos a continuación el listado de algunas de las medidas que, de prosperar el proyecto (y ser considerado pertinente en la evaluación de tesis) podríamos agregar con el paso del tiempo:

- Solicitud del fiscal para solicitar la realización de extracción de información de equipos secuestrados pero no analizados.
- Solicitud del fiscal para realizar pericia informática (podría brindarse modelos para distintos tipos de dispositivos)
- Solicitud del fiscal para acceder a una cuenta de mail utilizando como herramienta un dispositivo celular secuestrado.
- Modelo de Solicitud MLAT
- Solicitud para autorizar el desbloqueo compulsivo de datos informáticos.

- Solicitud de un agente encubierto informático combinado con registro remoto (utilizando el agente encubierto para realizar prácticas de ingeniería social).
- Entre otras.

5.2. Mejoras en el desarrollo de sistema y diseño

La versión 1.0. del sistema ha sido desarrollado con una combinación de tecnología de Google, donde inicialmente utilizamos Forms, sumado con el desarrollo y seteo de una extensión que permite procesar los datos, y combinarlos con escritos pre formateados existentes en Google Docs.

Actualmente, la tecnología desarrollada sólo nos permite reemplazar una palabra clave determinada, por una respuesta preseteada. Por ejemplo, el término <<plazo>>, es reemplazado por: “diez (10) días”, que es la opción seleccionada por el usuario.

A futuro, consideramos que sería importante generar un nuevo desarrollo a medida, con alguna tecnología que permita mayor nivel de granularidad entre las opciones brindadas al usuario, y que permita que al finalizar el circuito, se pueda descargar el documento generado sin necesidad de enviarse al correo electrónico (que el envío sea opcional).

Por otro lado, destacamos que actualmente hemos pretendido que el formulario diseñado, junto con sus preguntas, resulten lo más sencillos posible, a fin de facilitar su comprensión y por lo tanto, su utilización. Toda vez que como hemos advertido al comienzo de la propuesta, los destinatarios son personas de la Fiscalía o de las fuerzas de seguridad al mando de la investigación o incluso el propio Juez/a (dependiendo de la jurisdicción o el modelo penal utilizado).

A modo de mejora, la utilización de Google Forms limita mucho las opciones disponibles, así como la forma de mostrar la información, textos, etc, por lo que consideramos que podría mejorarse mucho a nivel de diseño y experiencia de usuario.

5.4. Incorporación de inteligencia artificial

A partir del entrenamiento de los distintos modelos, consideramos que a futuro sería posible la implementación de inteligencia artificial al proyecto que permita mejoras en distintos aspectos:

5.4.1. Procesamiento del lenguaje natural (NLP)

Utilizar NLP para mejorar la capacidad del sistema de entender y procesar la información proporcionada por el usuario. Esto puede incluir la capacidad de analizar y comprender los textos legales relevantes, así como los datos ingresados por el usuario en lenguaje natural.

5.4.2. Generación de texto automática basado en legislación aplicable

Implementar algoritmos de generación de texto automática para mejorar los modelos de escritos generados por el sistema. Esto podría incluir la generación de argumentos legales sólidos basados en la información proporcionada por el usuario y en la legislación pertinente (por ejemplo, preguntarle al usuario en qué País o Estado se encuentra, y generarle el escrito basado en la normativa aplicable).

5.4.3. Asistente virtual

Crear un asistente virtual basado en inteligencia artificial que guíe al usuario a través del proceso de selección de medidas de investigación y la recopilación de datos necesarios. Este asistente podría utilizar técnicas de aprendizaje automático para mejorar sus recomendaciones y respuestas a lo largo del tiempo.

5.4.4. Análisis predictivo

Implementar modelos de análisis predictivo para identificar patrones y tendencias en las solicitudes de medidas de investigación y en los casos de delitos informáticos. Esto podría ayudar a predecir qué medidas son más efectivas en diferentes situaciones y proporcionar recomendaciones más precisas a los usuarios.

5.4.5. Personalización del servicio:

Utilizar algoritmos de aprendizaje automático para personalizar la experiencia del usuario en función de sus necesidades y preferencias. Esto podría incluir la capacidad de recomendar medidas de investigación específicas en función del tipo de delito informático y del contexto del caso.

Por ejemplo, que el usuario pueda comentar el caso concreto, el tipo de datos con el que cuenta (por ejemplo, una dirección IP, un número de teléfono, una cuenta de instagram, etc.) y que, basado en aprendizaje previo, el sistema pueda realizarle una propuesta concreta de una o más medidas o técnicas especiales de investigación para su caso.

5.4.6. Detección de comportamientos dañinos

Implementar algoritmos de detección de fraudes o comportamientos dañinos o abusivos en el uso del sistema. Esto podría incluir la detección de comportamientos sospechosos o inusuales por parte de los usuarios.

5.4.7. Mejora continua

Utilizar técnicas de aprendizaje automático para recopilar datos sobre el uso del sistema y la efectividad de las medidas de investigación propuestas. Podríamos utilizar estos datos para mejorar continuamente el sistema y proporcionar mejores recomendaciones a los usuarios en el futuro.

5.5. Inclusión de normativa procesal penal aplicable

De la misma forma que se realiza con el proyecto ODILA en materia de derecho penal de fondo aplicable a cada jurisdicción, donde el usuario selecciona su jurisdicción y el tipo penal del cuál fue víctima, y el sistema le informa si el hecho reportado se encuentra o no tipificado, y en caso positivo, le indica el artículo y texto completo que podría (en principio) aplicarse al caso.

Bajo esta misma lógica, a futuro nuestro sistema podría consultar al usuario si pertenece a algunas de las jurisdicciones incluídas en el estudio realizado en la tesis (que a futuro podría ampliarse a otros países) y consultar sobre la medida de interés. Entre la información brindada (que hoy es genérica y no hace referencia a ningún sistema jurídico concreto), el sistema podría informar si en dicha jurisdicción, la medida de interés (por ejemplo, el agente encubierto digital) posee algún tipo de regulación aplicable o parcialmente aplicable.

Incluso, en combinación con las ideas propuestas para aplicar inteligencia artificial, a futuro podríamos lograr que el escrito generado, tenga en cuenta la normativa existente, logrando mayor solidez en cuanto a los argumentos de solicitud de la medida o técnica especial de investigación.

5.6. Mejoras a nivel de privacidad

Como hemos mencionado a lo largo del desarrollo, la confidencialidad de la información y la privacidad de las personas es un tema de marcada importancia para nosotros.

Por este motivo, en esta versión preliminar se han tomado decisiones como las de no incluir datos personales en el escrito,a fin de minimizar la recolección de datos, en pos de aplicar en la medida de lo posible, el principio de privacidad por defecto.

En esta línea, actualmente el único dato personal real recolectado, es el correo electrónico al cuál se enviará el escrito solicitado, que si bien puede no dar ningún

indicio sobre la persona solicitante, también es posible que permita identificarlo o hacerlo identificable. Por eso, entre las mejoras a realizarse a futuro esperamos que el escrito pueda ser generado y ofrecido en línea, en formato pdf y formato editable sin necesidad de dejar ningún dato personal, a fin de preservar en la mayor medida posible, la privacidad del usuario.

6.0. Versión preliminar 1.0.

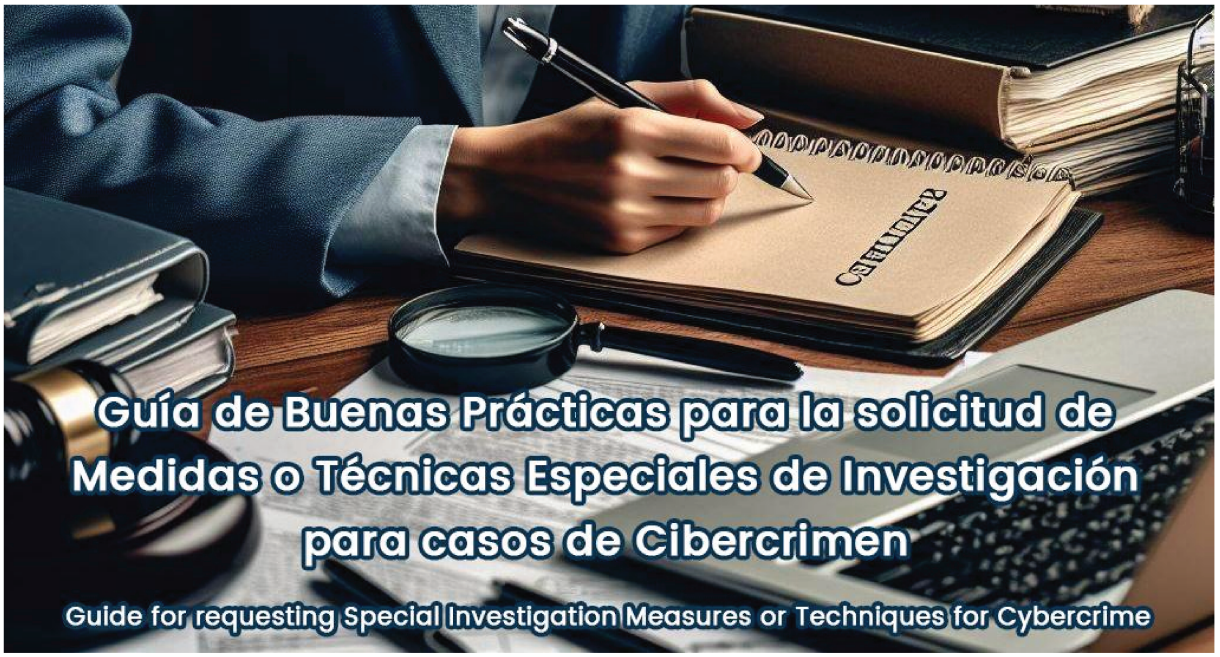
Como hemos afirmado en la introducción de este capítulo final, entre ser pesimistas o ser positivos, optamos por un término medio: ser realistas. Preferimos que hasta tanto cambie el viento y la normativa procesal penal en deuda sea efectivamente sancionada, podemos hacer algo al respecto.

Recordando que la misión del proyecto es proponer una Guía que pueda ser tenida en consideración a nivel internacional como una referencia para todas aquellas jurisdicciones que de momento, no poseen una adecuada regulación en el ámbito procesal penal relacionada a medidas o técnicas especiales de investigación sobre evidencia digital.

Entendiendo que este proyecto propone la construcción de una alternativa posible, que tenga como finalidad última aportar conocimiento tendiente a la obtención de información y elementos de convicción para descubrir o identificar a las personas involucradas en la comisión del delito informático, aportar pruebas al proceso sobre el delito investigado, teniendo siempre en cuenta la debida garantía de los derechos humanos y las libertades de las personas.

Por todo lo expuesto, proponemos ahora sí, como entrega final, la versión preliminar 1.0. de la “Guía de Buenas Prácticas sobre medidas o técnicas especiales de investigación para el cibercrimen”, que permita a todas aquellas jurisdicciones que aún no tienen normativa al respecto, poder tener un norte hacia donde caminar.

Sin más que agregar, y quedando siempre con la esperanza que nuestro aporte pueda sumar un granito de arena que nos permita, en definitiva, llevar adelante un combate eficaz contra la ciberdelincuencia.



Guía de Buenas Prácticas para la solicitud de Medidas o Técnicas Especiales de Investigación para casos de Cibercrimen

Guide for requesting Special Investigation Measures or Techniques for Cybercrime

Versión preliminar 1.0

Autor: Abog. Marcelo Temperini

1.0. Aspectos Generales

1.1. Alcance

La presente Guía de Buenas Prácticas tiene como principales públicos objetivo a aquellas personas que desarrollen sus actividades en el Ministerio Público Fiscal o en Fuerzas de Seguridad, e incluso, de Jueces o Juezas de Instrucción, dependiendo del país y de la forma de organización de la justicia (sistema acusatorio o inquisitivo).

1.2. Finalidad

Las medidas o técnicas especiales de investigación desarrolladas en esta Guía tienen por finalidad la obtención de información y elementos de convicción para descubrir o identificar a las personas involucradas en la comisión del delito, aportar pruebas al proceso sobre el delito investigado y, en su caso, prestar auxilio a autoridades extranjeras para estos mismos fines, teniendo siempre en cuenta la debida garantía de los derechos humanos y las libertades de las personas.

1.3. Principios aplicables

1.3.1. Principio de Excepcionalidad y Necesidad:

Las medidas o técnicas especiales de investigación podrán ordenarse cuando no estén a disposición de la investigación, en atención a sus características, otras medidas menos gravosas para los derechos fundamentales del investigado o encausado e igualmente útiles para el esclarecimiento del hecho, o cuando el descubrimiento o la comprobación del hecho investigado, la determinación de su autor o autores, la averiguación de su paradero, o la localización de los efectos del delito se vea gravemente dificultada sin el recurso a esta medida.

1.3.2. Principio de Especialidad:

El principio de especialidad implica que las medidas de investigación deben ser precisas y estar claramente delimitadas en su alcance, de modo que se respete la presunción de inocencia y se evite la intrusión injustificada en la esfera de intimidad de los individuos. De esta manera, al evaluar la pertinencia de una medida de investigación, se deben tener en cuenta no sólo los criterios de legalidad y competencia, sino también los principios de necesidad, proporcionalidad y respeto a los derechos fundamentales, garantizando así que la medida adoptada sea adecuada para la consecución de los fines de la justicia penal y que se ajuste a los estándares establecidos por el Estado de Derecho.

1.3.3. Principio de Proporcionalidad:

La medida o técnica especial de investigación sólo se considerará proporcionada cuando, tomadas en consideración todas las circunstancias del caso, el sacrificio de los derechos e intereses afectados no sea superior al beneficio que de su adopción resulte para el interés público y de terceros. Para la ponderación de los intereses en conflicto, se sugiere que la valoración del interés público se basará en la gravedad del hecho, su trascendencia social o el ámbito tecnológico de producción, la intensidad de los indicios existentes y la relevancia del resultado perseguido con la restricción del derecho.

1.3.4. Principio de razonabilidad:

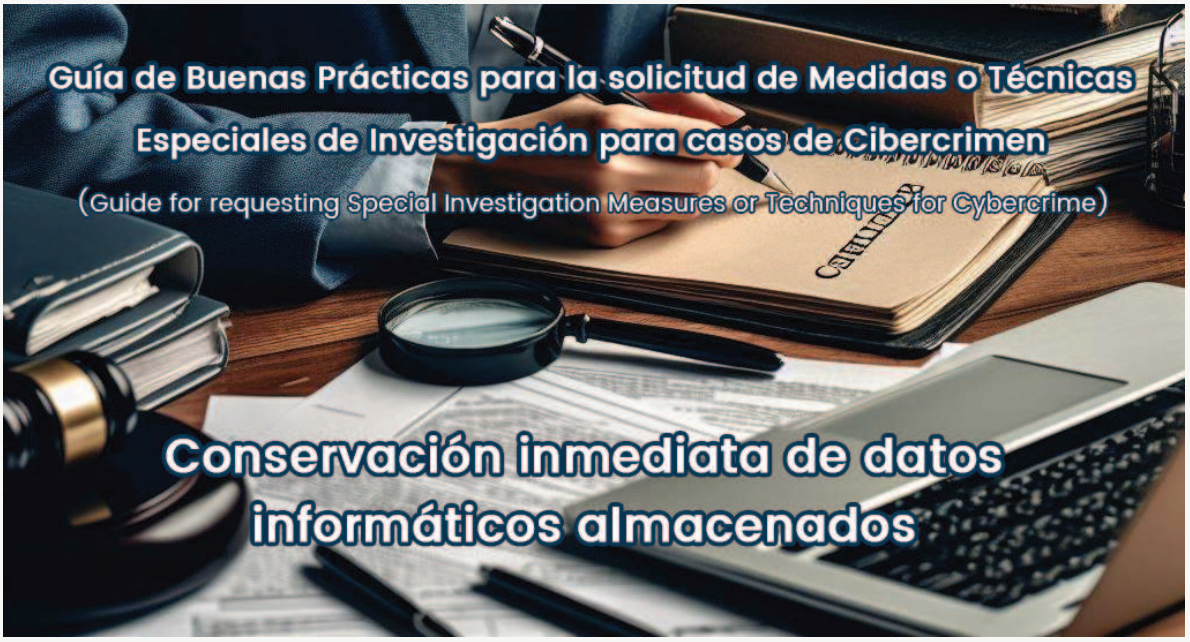
El principio de razonabilidad desempeña un papel fundamental en la garantía de un proceso justo y equitativo. Este principio establece que las decisiones judiciales y las actuaciones procesales deben estar fundamentadas en criterios lógicos y racionales, evitando arbitrariedades y garantizando el respeto a los derechos fundamentales de las partes involucradas.

En el contexto del proceso penal, la aplicación del principio de razonabilidad implica que las medidas adoptadas por los órganos jurisdiccionales, tales como la imposición de medidas cautelares, la valoración de pruebas y la imposición de sanciones, deben estar justificadas en base a la evidencia presentada y ser proporcionales a la gravedad del delito y a las circunstancias del caso concreto.

2.0. De las medidas o técnicas especiales de investigación

2.1. Listado de medidas o técnicas especiales de investigación que no necesitan autorización judicial

A continuación, se realizará una descripción de una serie de medidas o técnicas especiales de investigación que, de acuerdo a nuestro estudio, no requieren autorización judicial previa para poder ser diligenciadas. El listado se compone de las siguientes medidas:



2.1.1. Conservación inmediata de datos informáticos almacenados

2.1.1.1. ¿En qué consiste?

- Esta medida consiste en ordenar a una persona física o jurídica (generalmente un proveedor de servicios) el aseguramiento de datos informáticos concretos almacenados (pueden ser datos de contenido, tráfico, abonado o de cualquier tipo) en un sistema informático o en un dispositivo de almacenamiento informático que esté bajo su disposición o control y para el que tenga legítimo acceso, cuando los datos puedan ser de utilidad en una investigación concreta y tenga motivos para sospechar que éstos pueden ser alterados o suprimidos o de cualquier forma dejar de estar disponibles.

2.1.1.2. ¿Quién puede solicitar la medida?

La respuesta depende de lo establecido normativamente por cada jurisdicción, pero por lo general y de acuerdo a nuestro estudio de derecho comparado internacional, se considera que para esta medida o técnica especial de investigación:

- No necesita de previa autorización judicial para poder ordenarse
- Puede ser solicitada por el o la Fiscal a cargo de la investigación, o alternativamente, por la Fuerza de Seguridad encargada de la misma, sobre todo en casos donde se considere que corre riesgo perder información de interés.

2.1.1.3. ¿Qué límites deberían especificarse en la orden?

- El detalle de los datos que se pretenden asegurar o la categoría de datos (si son datos de abonado, de tráfico o de contenido o datos no relacionados con una comunicación electrónica).
- La modalidad técnica de la conservación (si es que se tiene conocimiento de la misma).
- Duración de la medida, que por lo general no puede exceder de noventa (90) días, prorrogables por igual período si se mantienen los motivos que fundamentaron la orden.
- La necesidad del secreto o confidencialidad, en el caso que se considere necesario de acuerdo al caso concreto.

2.1.1.4. Notas adicionales

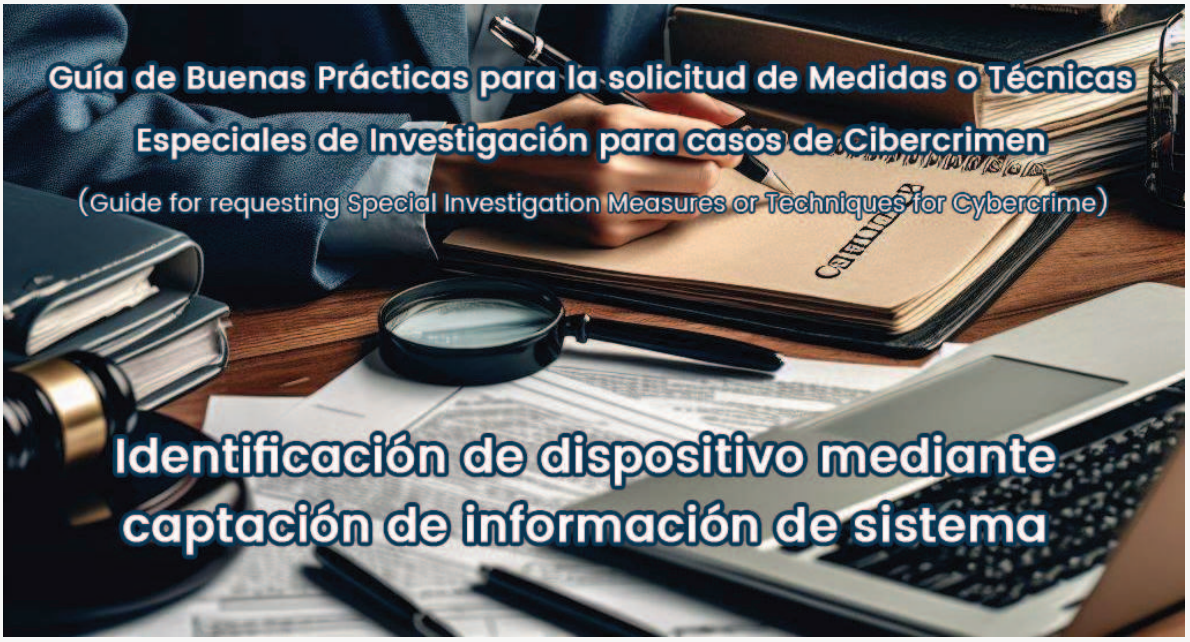
- Recordar que esta medida sólo permite el aseguramiento de los datos. No autoriza a ordenar la entrega de dichos datos. Ordenar la entrega de datos es una medida diferente.
- Considerar que muchos de los principales proveedores de servicios, cuentan con un portal propio donde pueden acceder las fuerzas de seguridad para canalizar este tipo de pedidos de forma electrónica, a través de formularios propios de cada empresa.

2.1.1.5. ¿Qué obtendría de esta solicitud?

- Una confirmación acerca de que los datos de interés, han sido resguardados adecuadamente por un tiempo determinado. Esto significa que podría avanzar a diligenciar una medida de obtención de datos.

2.1.1.6. Un ejemplo concreto del uso de esta medida o técnica especial de investigación

- Podría ser un caso donde la Fiscalía se encuentra investigando información existente sobre un perfil en una red social; una grabación de video de una fecha u horario determinado existente en un sistema de videovigilancia interno; información de un correo electrónico existente en un proveedor de servicios; entre otros. En los casos mencionados, podría existir el riesgo que, de no conseguir la medida que me permita el acceso a los datos de interés a tiempo, la información podría desaparecer, ya sea de forma voluntaria (porque el usuario borró la información) o automáticamente, como en el caso de las cámaras de seguridad, que cada cierto tiempo van pisando sus grabaciones.



2.1.2. Identificación de dispositivo mediante captación de información de sistema

2.1.2.1. ¿En qué consiste?

- Esta técnica consiste en la recolección, procesamiento y análisis de un conjunto de información que expone un dispositivo o sistema determinado al conectarse a un servidor controlado por el investigador.
- Entre la información que puede ser captada de la interacción con un sistema o dispositivo, podemos mencionar el sistema operativo utilizado, su versión, navegador de internet utilizado, plugins instalados, fuentes instaladas en dicho sistema, resolución de pantalla utilizada por el dispositivo, dirección IP pública utilizada por la conexión a internet, modelo del dispositivo celular utilizado (en el caso que la conexión sea realizada desde un celular) hasta incluso, en algunos casos, la ubicación geográfica de la persona conectada.
- Del conjunto de todos los datos que se puedan recolectar del dispositivo de interés, usualmente se procede a realizar un agrupamiento de este conjunto de datos, generando una "huella digital" del dispositivo, que podrá ser de utilidad para la investigación en curso.

2.1.2.2. ¿Quién puede solicitar la medida?

La respuesta depende de lo establecido normativamente por cada jurisdicción, pero por lo general y de acuerdo a nuestro estudio de derecho comparado internacional, se considera que para esta medida o técnica especial de investigación:

- Depende del alcance de la medida. Para la recolección de ciertos datos de sistema no se necesita de previa autorización judicial para poder ordenarse. En el caso de que la técnica deseada implique algún tipo de interacción con cuentas o la persona sospechada, recomendamos solicitar autorización judicial.
- Puede ser solicitada por el o la Fiscal a cargo de la investigación, o alternativamente, por la Fuerza de Seguridad encargada de la misma, sobre todo en casos donde se considere que corre riesgo perder información de interés.

2.1.2.3. ¿Qué límites deberían especificarse en la orden?

- Debería especificarse el usuario / número de línea / dispositivo de interés, con el cuál se va a interactuar.
- En caso de ser posible, debería especificarse la técnica particular que se utilizaría para la obtención de la información (por ejemplo, a través de Browser Fingerprinting, CANVAS Fingerprinting, WEBRTC, etc.)
- Debería especificarse las medidas de seguridad de la información que serían aplicadas para poder garantizar la integridad y confidencialidad de la información obtenida.
- Debería especificarse la Fuerza de Seguridad autorizada (hasta incluso, en el caso de ser posible, el o la agente de dicha fuerza que llevaría adelante la ejecución de la técnica).

2.1.2.4. Notas adicionales

- Considerar que la autorización de la presente medida, implica que debería existir la posibilidad de algún tipo de interacción con la persona investigada, por lo que sólo será de utilidad para una determinada gama de casos. Su utilidad sólo será para casos donde existe la posibilidad de algún tipo de intercambio como Whatsapp, Redes Sociales, Correo Electrónico, entre otros tipos de comunicaciones.
- La ejecución de la medida, dependiendo de la técnica utilizada, puede o no necesitar algún tipo de interacción con el usuario del sistema. En algunos casos, es posible obtener respuestas automáticas (caso de obtención de información sobre servicios funcionando sobre una determinada IP por ejemplo). En otros casos, es posible que sea necesaria la interacción con el usuario del sistema o dispositivo (por ejemplo, que ingrese a ver una imagen, o que haga click en algún hipervínculo). En estos últimos casos, puede ser de utilidad combinar esta medida con el agente encubierto informático.

2.1.2.5. ¿Qué obtendría de esta solicitud?

- Una autorización que permita ejecutar una o más técnicas de identificación de dispositivos, a fin de conseguir información que pueda ser de interés para la investigación en curso.

2.1.2.6. Un ejemplo concreto del uso de esta medida o técnica especial de investigación

- Ante el caso de una investigación de una banda dedicada a las estafas bancarias, sería posible (en el caso de contar con la tecnología necesaria) realizar la captura de datos como el IMSI o IMEI de determinadas comunicaciones electrónicas.



2.1.3. Mandato de comunicación de datos de abonado

2.1.3.1. ¿En qué consiste?

- Consiste en ordenar a una persona física o jurídica la entrega de datos de abonado (datos básicos de suscripción o BSI), que se encuentren alojados en un dispositivo de almacenamiento o sistema informático que esté bajo su poder o control y al que pueda acceder legítimamente, siempre que los datos solicitados se vinculen con la investigación de un delito concreto de su competencia.

2.1.3.2. ¿Quién puede solicitar la medida?

La respuesta depende de lo establecido normativamente por cada jurisdicción, pero por lo general y de acuerdo a nuestro estudio de derecho comparado internacional, se considera que para esta medida o técnica especial de investigación:

- No requiere de previa autorización judicial, toda vez que los datos solicitados no forman parte de una comunicación privada.
- Puede ser solicitada por el o la Fiscal a cargo de la investigación, o alternativamente, por la Fuerza de Seguridad encargada de la misma, sobre todo en casos donde se considere que corre riesgo perder información de interés.

2.1.3.3. ¿Qué límites deberían especificarse en la orden?

- El detalle o dato de abonado que se tenga identificado de interés (nombre de usuario, id de conexión, número de cliente, etc.). En el caso que el dato que se tiene sea una dirección IP, debe determinarse con precisión la fecha y horario exacto (incluyendo huso horario) de las conexiones investigadas.
- En el caso que se tenga certeza, el detalle de los datos que se pretenden que se entreguen (por ejemplo, mail o teléfono indicados en la suscripción del servicio).
- La modalidad técnica de la entrega de datos (por ejemplo, a través de un correo electrónico)
- La necesidad del secreto o confidencialidad, en el caso que se considere necesario de acuerdo al caso concreto.

2.1.3.4. Notas adicionales

- Considerar que muchos de los principales proveedores de servicios, cuentan con un portal propio donde pueden acceder las fuerzas de seguridad para canalizar este tipo de pedidos de forma electrónica, a través de formularios propios de cada empresa.
- En caso que sea necesaria la cooperación internacional, es importante considerar la existencia del Acuerdo de Cooperación Interinstitucional entre los Ministerios Públicos miembros de la Asociación Iberoamericana de Ministerios Públicos (AIAMP), que plasma el compromiso de cooperar de manera directa en el marco de investigaciones judiciales, al establecer en su cláusula tercera, que los Ministerios Públicos de los países que pertenecen a la red, en su carácter de autoridades competentes, deben cooperar entre sí intercambiando información de manera directa en el marco de investigaciones.

2.1.3.5. ¿Qué obtendría de esta solicitud?

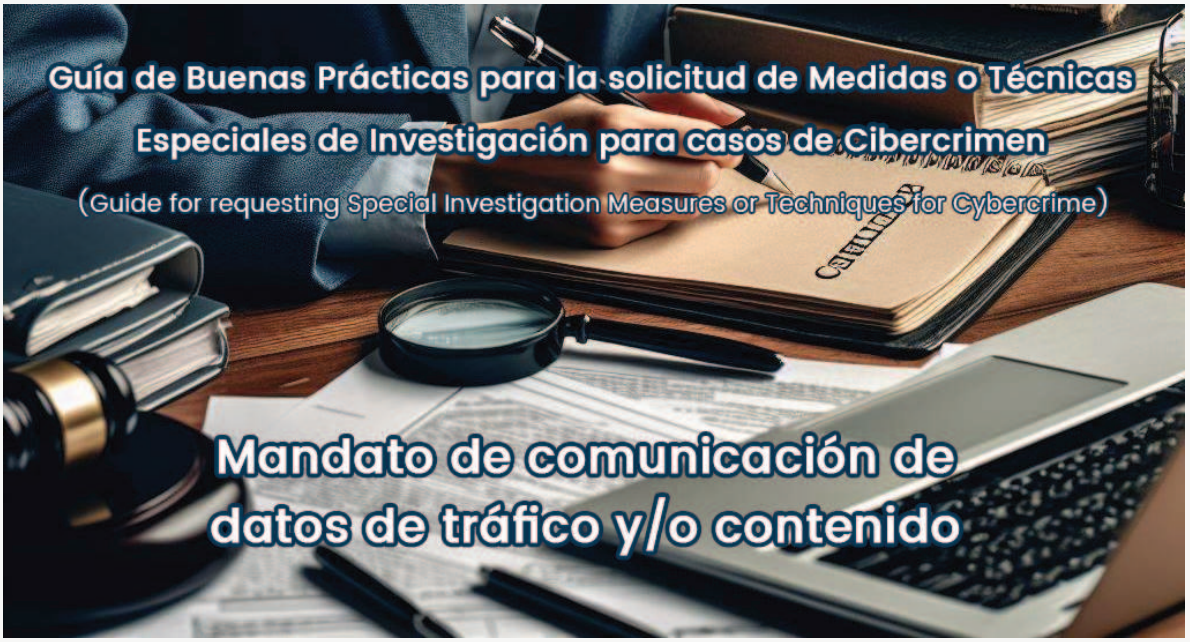
- La entrega efectiva de los datos de abonado que han sido solicitados.

2.1.3.6. Un ejemplo concreto del uso de esta medida o técnica especial de investigación

- Ante el caso de una investigación por daño informático, donde se tiene el dato de la dirección IP utilizada por la persona autora del delito, esta medida tendría por finalidad exigir al ISP pertinente (consultar en whois para saber a que ISP pertenece dicha dirección IP), que informe los datos de abonado (BSI) del cliente al cuál se le asignó dicha IP en una fecha y horario exacto (tener precisión en este aspecto).

2.2. Listado de medidas o técnicas especiales de investigación que necesitan autorización judicial

A continuación, se realizará una descripción de una serie de medidas o técnicas especiales de investigación que, de acuerdo a nuestro estudio, **requieren autorización judicial previa para poder ser diligenciadas**. El listado se compone de las siguientes medidas:



2.2.1. Mandato de comunicación de datos de tráfico y/o contenido

2.2.1.1. ¿En qué consiste?

- Consiste en ordenar a una persona física o jurídica la entrega de datos de tráfico o de contenido, que se encuentren alojados en un dispositivo de almacenamiento o sistema informático que esté bajo su poder o control y al que pueda acceder legítimamente, siempre que los datos solicitados se vinculen con la investigación de un delito concreto de su competencia.

2.2.1.2. ¿Quién puede solicitar la medida?

La respuesta depende de lo establecido normativamente por cada jurisdicción, pero por lo general y de acuerdo a nuestro estudio de derecho comparado internacional, se considera que para esta medida o técnica especial de investigación:

- Requiere de autorización judicial, toda vez que los datos solicitados forman parte e incluso, podrían incluir el contenido de una comunicación privada.
- El o la Fiscal a cargo de la investigación debe enviar la solicitud al Juez o Jueza de Garantías (o que corresponda de acuerdo a la jurisdicción) a fin de que autorice el libramiento de los oficios a los proveedores de servicios indicados. Los oficios ya autorizados, podrían ser diligenciados por alguna Fuerza de Seguridad autorizada también para recibir la información requerida.

2.2.1.3. ¿Qué límites deberían especificarse en la orden?

- El detalle o dato de abonado que se tenga identificado de interés (nombre de usuario, id de conexión, número de cliente, etc.).
- En el caso que el dato que se tiene sea una dirección IP, debe determinarse con precisión la fecha y horario exacto (incluyendo huso horario) de las conexiones investigadas.
- En el caso que se tenga certeza, el detalle de los datos que se pretenden que se entreguen (por ejemplo, mail o teléfono indicados en la suscripción del servicio).
- La modalidad técnica de la entrega de datos (por ejemplo, a través de un correo electrónico)
- La necesidad del secreto o confidencialidad, en el caso que se considere necesario de acuerdo al caso concreto.

2.2.1.4. Notas adicionales

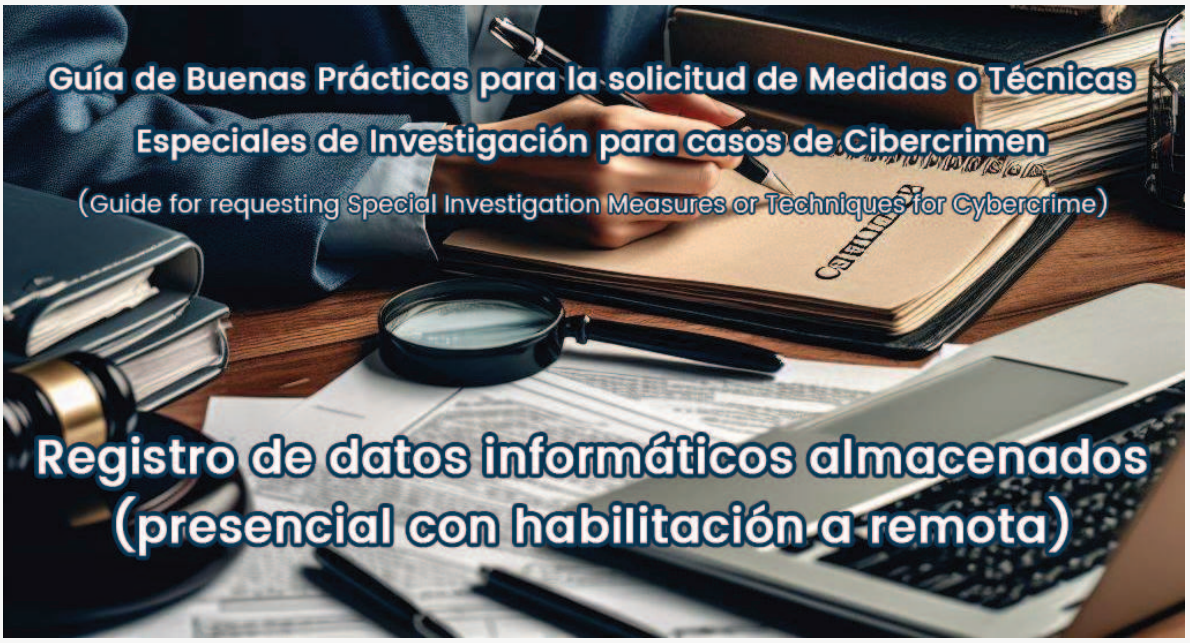
- Considerar que muchos de los principales proveedores de servicios, cuentan con un portal propio donde pueden acceder las fuerzas de seguridad para canalizar este tipo de pedidos de forma electrónica, a través de formularios propios de cada empresa.
- En caso que sea necesaria la cooperación internacional (depende del proveedor de servicios), es importante considerar la existencia del Acuerdo de Cooperación Interinstitucional entre los Ministerios Públicos miembros de la Asociación Iberoamericana de Ministerios Públicos (AIAMP), que plasma el compromiso de cooperar de manera directa en el marco de investigaciones judiciales, al establecer en su cláusula tercera, que los Ministerios Públicos de los países que pertenecen a la red, en su carácter de autoridades competentes, deben cooperar entre sí intercambiando información de manera directa en el marco de investigaciones.

2.2.1.5. ¿Qué obtendría de esta solicitud?

- La efectiva entrega de los datos de tráfico o de contenidos solicitados.

2.2.1.6. Un ejemplo concreto del uso de esta medida o técnica especial de investigación

- Ante el caso de una investigación por extorsión vinculada con ransomware, donde la casilla de correo electrónico utilizada por la persona investigada estuviera en un proveedor de servicios, esta medida permitiría solicitar el acceso a dichos datos de contenido (correos electrónicos enviados, o mensajes existente en el sistema de chat), a fin de poder encontrar elementos de interés para la investigación en curso.



2.2.2. Registro de datos informáticos almacenados (presencial con habilitación a remota)

2.2.2.1. ¿En qué consiste?

- Consiste en una medida que autoriza a la obtención utilizando la fuerza pública (generalmente en el marco de un allanamiento) de datos informáticos que se encuentren alojados en un dispositivo de almacenamiento o sistema informático que esté bajo poder o control de una persona física o jurídica. Esta medida normalmente incluye el acceso, búsqueda de información de interés en los dispositivos, y su extracción (copia) debidamente preservada (protocolos forenses).

2.2.2.2. ¿Quién puede solicitar la medida?

La respuesta depende de lo establecido normativamente por cada jurisdicción, pero por lo general y de acuerdo a nuestro estudio de derecho comparado internacional, se considera que para esta medida o técnica especial de investigación:

- Requiere de autorización judicial, toda vez que los datos informáticos a los que se pretenden acceder (por ejemplo en un equipo informático, dispositivo celular, etc.), podrían contener comunicaciones privadas, afectando garantías constitucionales.
- El o la Fiscal a cargo de la investigación debe enviar la solicitud al Juez o Jueza de Garantías (o que corresponda de acuerdo a la jurisdicción) a fin de que autorice la posibilidad del registro. El registro propiamente dicho, generalmente es delegado a alguna Fuerza de Seguridad o Unidad especializada en informática forense.

2.2.2.3. ¿Qué límites deberían especificarse en la orden?

- La identificación concreta del propietario de los equipos o sistemas donde se encuentra la información de interés. (persona física o jurídica).
- La descripción del hecho objeto de investigación y la identidad del investigado o de cualquier otro afectado por la medida, siempre que tales datos resulten conocidos.
- La orden judicial que autorice la medida deberá fundamentar su necesidad, razonabilidad y proporcionalidad (establecidos en la sección 1.3 de la presente Guía (o en caso de existir, en el Código Procesal Local aplicable), justificando especialmente la ponderación de su - utilidad con relación a la afectación de derechos fundamentales involucrados, la gravedad del hecho investigado y que no existen medios menos intrusivos de la intimidad del imputado que resulten útiles para alcanzar los mismos fines probatorios.
- En caso de existir, los indicios de criminalidad que se hayan puesto de manifiesto durante la investigación previa a la solicitud de autorización del acto de injerencia.
- El detalle de los patrones de búsqueda, a fin de garantizar la relevancia y pertinencia de los datos recolectados en el marco de esta medida.
- La Fuerza de Seguridad que estará autorizada para coordinar y recibir el envío de la información solicitada.

2.2.2.4. Notas adicionales

- Considerar que la presente medida en la mayoría de los casos (información almacenada de forma local) implica la existencia previa de una autorización de allanamiento y registro domiciliarios. No obstante podría darse el caso donde se tenga conocimiento que la información se encuentra alojada en un servicio en la nube, por lo que realizar el allanamiento no tendría sentido, excepto que algunos de los equipos autorizados al acceso se encuentren en el domicilio de interés.
- Considerar que normalmente este tipo de medidas implica una recolección de datos "en caliente" (acceso y extracción de datos de sistemas en tiempo real) por lo que deben reforzarse las medidas que puedan garantizar las operaciones técnicas realizadas, a fin de evitar cuestionamientos.

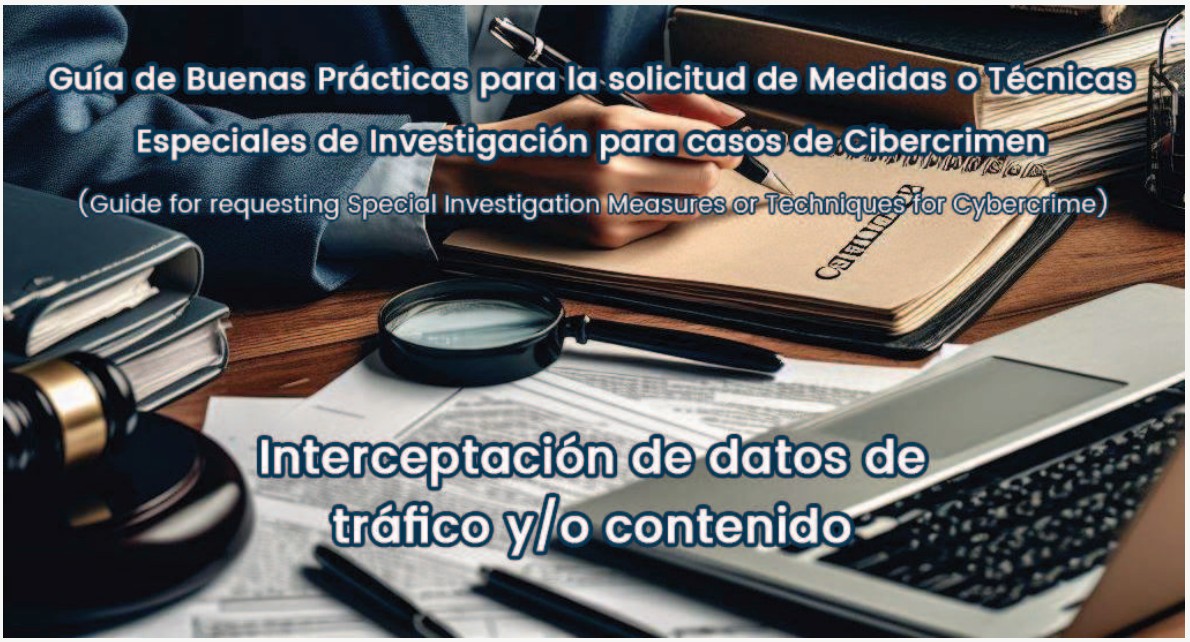
- En el caso que el personal idóneo para realizar la recolección no pueda asistir en el marco del allanamiento practicado, existe la posibilidad de solicitar se habilite la conexión remota (asistida localmente por alguien de la fuerza de seguridad) del profesional de la informática forense, a fin de que pueda realizar la misma extracción pero sin necesidad de encontrarse presente físicamente en el marco del allanamiento.

2.2.2.5. ¿Qué obtendría de esta solicitud?

- La autorización para acceder a los dispositivos que contienen información almacenada por parte de la persona de interés. Logrado el acceso, estaría autorizado a realizar la búsqueda y copia de la información de interés para la investigación.
- Importante: Recordar que la simple autorización de registro o mandato de datos, no permite ni autoriza el secuestro del dispositivo que contiene los datos, de la misma forma que la autorización al secuestro de los dispositivos, no implica la autorización al acceso y copia de los datos.

2.2.2.6. Un ejemplo concreto del uso de esta medida o técnica especial de investigación

- Ante el caso de una investigación por extorsión vinculada con la denegación de servicios de una víctima (por ejemplo, un ataque de ransomware), donde la casilla de correo electrónico utilizada por la persona investigada estuviera en un proveedor de servicios, esta medida permitiría solicitar el acceso a dichos datos de contenido (correos electrónicos enviados, o mensajes existente en el sistema de chat), a fin de poder encontrar elementos de interés para la investigación en curso.



2.2.3. Interceptación de datos de tráfico y/o contenido

2.2.3.1. ¿En qué consiste?

- Consiste en una medida que autoriza la intervención de comunicaciones electrónicas, ya sea de forma autónoma (realizado por la propia Fuerza de Seguridad) o bien a través de la cooperación de uno o más proveedores de servicios, para impedirlas o conocerlas.

2.2.3.2. ¿Quién puede solicitar la medida?

La respuesta depende de lo establecido normativamente por cada jurisdicción, pero por lo general y de acuerdo a nuestro estudio de derecho comparado internacional, se considera que para esta medida o técnica especial de investigación:

- Requiere de autorización judicial, toda vez que los datos informáticos a los que se pretenden acceder son comunicaciones privadas, afectando garantías constitucionales.
- El o la Fiscal a cargo de la investigación debe enviar la solicitud al Juez o Jueza de Garantías (o que corresponda de acuerdo a la jurisdicción) a fin de que autorice la posibilidad de interceptación de los datos. La interceptación propiamente dicha, generalmente es realizada directamente por el proveedor de servicios. Alternativamente, una fuerza de seguridad especializada, si cuenta con las herramientas y tecnologías adecuadas, también podría llevar a cabo una interceptación de datos.

2.2.3.3. ¿Qué límites deberían especificarse en la orden?

- La identificación de la/s persona/s o comunicación/es concreta/s que se desea intervenir.
- Deberá determinarse si se solicita la interceptación de datos de tráfico y/o de contenido, así como si se desea que la intervención sea sobre datos en tránsito o sobre los datos almacenados.
- La exposición detallada de las razones que justifiquen la necesidad de la medida de acuerdo a los principios rectores establecidos en la sección 1.3 de la presente Guía (o en caso de existir, en el Código Procesal Local aplicable). En caso de existir, los indicios de criminalidad que se hayan puesto de manifiesto durante la investigación previa a la solicitud de autorización del acto de injerencia.
- Se deberá indicar que los medios técnicos utilizados para su interceptación o captación aseguren la integridad de los registros (en el caso que se tenga conocimiento de los mismos).
- En el caso de ser posible, deberá determinarse uno o más interlocutores de interés, a fin de resguardar la privacidad de comunicaciones que no sean de interés para la causa.
- La duración de la medida. En el caso que sea una medida que proponga la intervención de comunicaciones futuras, la intervención solicitada podrá tener un máximo de hasta treinta (30) días, los que podrán ser renovados mediante decreto fundado y cuando existan motivos que los justifiquen.
- La Fuerza de Seguridad que estará autorizada para ejecutar la medida, y en caso de ser posibles, las personas especializadas que podrán ejecutar las mismas.
- Opcionalmente, en caso de ser necesaria la cooperación de un proveedor de servicios, se sugiere ordenar mantener el secreto de la ejecución de la medida, a fin de evitar que se frustre.

2.2.3.4. Notas adicionales

- Considerar que muchos de los principales proveedores de servicios, cuentan con un portal propio donde pueden acceder las fuerzas de seguridad para canalizar este tipo de pedidos de forma electrónica, a través de formularios propios de cada empresa.
- Recordar que está generalmente está prohibida bajo sanción de nulidad, la intervención de comunicaciones electrónicas de cualquier tipo que implique la participación de los abogados defensores y de los demás letrados con intervención en la causa.
- En caso que sea necesaria la cooperación internacional (depende del proveedor de servicios), es importante considerar la existencia del Acuerdo de Cooperación Interinstitucional entre los Ministerios Públicos miembros de la Asociación Iberoamericana de Ministerios Públicos (AIAMP), que plasma el compromiso de cooperar de manera directa en el marco de investigaciones judiciales, al establecer en su cláusula tercera, que los Ministerios Públicos de los países que pertenecen a la red, en su carácter de autoridades competentes, deben cooperar entre sí intercambiando información de manera directa en el marco de investigaciones. En Argentina sugerimos recurrir a la Red de Cooperación 24/7 coordinada por la UFECI, a cargo del Dr. Horacio Azzolin.
- En caso de existir la posibilidad de que la intervención de las comunicaciones sea realizada por la propia Fuerza de Seguridad, se recomienda encargar la tarea a auxiliares de la justicia especializados en recolección de evidencia digital (usualmente peritos informáticos).
- En el caso que sea necesario el auxilio y cooperación de un proveedor de servicios de comunicación o internet (CSP o ISP), autorizada la medida, deberá diligenciar la medida a través de los canales

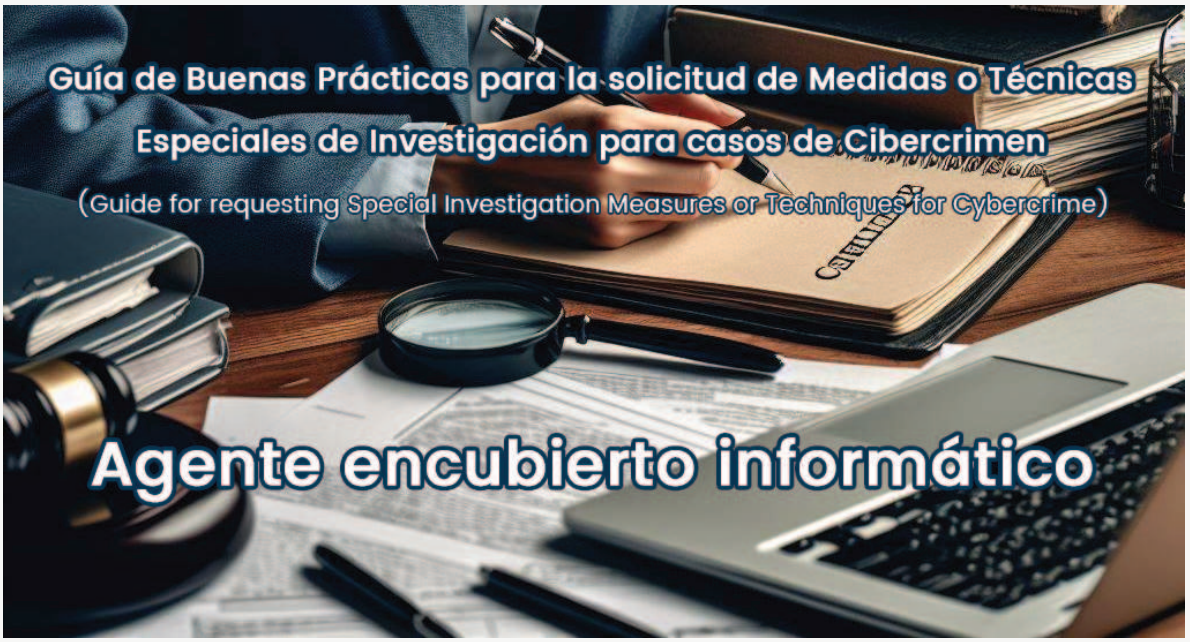
autorizados para las mismas. Se recomienda buscar si el proveedor de servicios de interés, posee un portal de cooperación para fuerzas de la Ley, a través del cuál agilizar el trámite de los pedidos.

2.2.3.5. ¿Qué obtendría de esta solicitud?

- La autorización para interceptar o recolectar las comunicaciones electrónicas de la persona de interés.

2.2.3.6. Un ejemplo concreto del uso de esta medida o técnica especial de investigación

- Ante el caso de una investigación por estafas informáticas, se detecta que la banda dedicada a la comisión de dichos delito, utiliza una serie de cuentas de redes sociales que simulan ser de entidades bancarias reconocidas, así como una serie de sitios de phishing que son utilizados como medios para recolectar los datos bancarios, que son generados desde una dirección IP determinada. Ante este tipo de casos, la medida de interceptación de comunicaciones electrónicas podría ser de utilidad, tanto para poder acceder a comunicaciones electrónicas almacenadas (en los usuarios de las redes sociales), así como para obtener los datos de tráfico y de contenido de las actividades realizadas por el usuario investigado de generar y poner a disposición los sitios web falsos.



2.2.4. Agente encubierto informático

2.2.4.1. ¿En qué consiste?

- Esta medida consiste en autorizar a un funcionario de las fuerzas de seguridad o miembro del Ministerio Público Fiscal, que previo prestar su consentimiento, oculte o utilice un perfil o identidad digital encubierto, interactúe y se relacione digitalmente a través de tecnologías de la información y de la comunicación con el objeto de: identificar o detener a los autores, partícipes o encubridores de un delito; impedir la consumación de un delito; o para reunir información o elementos de prueba necesarios para la investigación.

2.2.4.2. ¿Quién puede solicitar la medida?

La respuesta depende de lo establecido normativamente por cada jurisdicción, pero por lo general y de acuerdo a nuestro estudio de derecho comparado internacional, se considera que para esta medida o técnica especial de investigación:

- Requiere de autorización judicial, toda vez que la ejecución de la medida implica un nivel alto de injerencia s los derechos de la o las personas afectadas, ya que implica ocultar la verdadera identidad del agente, simular otra identidad, hasta incluso, el envío o compra de material ilícito, todo con la finalidad de conseguir ingresar en un ámbito de confianza de la banda.
- El o la Fiscal a cargo de la investigación debe enviar la solicitud al Juez o Jueza de Garantías (o que corresponda de acuerdo a la jurisdicción) a fin de que autorice la posibilidad de utilización de esta

figura. La ejecución práctica de esta figura, generalmente es delegada a una fuerza de seguridad especializada, que debe permanecer siempre bajo el control de la Unidad Fiscal solicitante.

2.2.4.3. ¿Qué límites deberían especificarse en la orden?

- La orden judicial que autorice la medida deberá fundamentar su necesidad, razonabilidad y proporcionalidad (establecidos en la sección 1.3 de la presente Guía o en caso de existir, en el Código Procesal Local aplicable), justificando especialmente la ponderación de su utilidad con relación a la afectación de derechos fundamentales involucrados, la gravedad del hecho investigado y que no existen medios menos intrusivos de la intimidad del imputado que resulten útiles para alcanzar los mismos fines probatorios.
- La descripción del hecho objeto de investigación o de cualquier otro afectado por la medida, siempre que tales datos resulten conocidos.
- En el caso de ser posible, deberá designarse el o los perfiles o identidades digitales falsas que estarán autorizadas dentro de la medida de investigación.
- Deberá ordenarse el control de la medida, por parte de la Fiscalía a cargo, de registrar toda la información necesaria respecto a los perfiles o identidades falsas, sistemas informáticos en los que se utilizarán, claves de acceso validadas y actividad concreta a desarrollar.
- En los casos donde se considere necesario, el Juez de Garantías podrá autorizar que, durante la investigación encubierta, se intercambien archivos o contenidos ilícitos, se compren o vendan bienes, activos digitales o servicios, se participe de foros o grupos o cualquier actividad en entornos digitales dirigida a identificar a los responsables de los hechos ilícitos investigados.
- La medida será autorizada por el plazo estrictamente necesario para lograr la individualización de los autores, partícipes o encubridores, o para obtener y asegurar los medios de prueba necesarios para su prosecución.
- La actuación encubierta no podrá exceder de ciento ochenta (180) días a contar desde que la autorización otorgada por el Juez Penal sea notificada al Fiscal.

2.2.4.4. Notas adicionales

- En caso de ser posible, y con la finalidad de tener mayores probabilidades de éxito en la medida intentada, se sugiere que la Fuerza de Seguridad dedicada a la ejecución de este tipo de medidas, tenga previamente perfiles o identidades falsas ya generados, que sean creíbles para el objetivo buscado.
- Recomendamos tener en cuenta la implementación de medidas de seguridad de la información, que permitan probar la integridad de los intercambios mantenidos desde el perfil o identidad falsa, a fin de evitar potenciales cuestionamientos.

2.2.4.5. ¿Qué obtendría de esta solicitud?

- La autorización para utilizar un perfil o identidad falsa, a través de medios informáticos o electrónicos, que nos permita interactuar con una o más personas de interés a fin de obtener información de interés para el delito investigado.

2.2.4.6. Un ejemplo concreto del uso de esta medida o técnica especial de investigación

- Ante el caso de una investigación por un caso de grooming, un agente de una fuerza de seguridad podría solicitar esta medida, a fin de utilizar un perfil falso de un menor de edad, de una determinada red social (por ejemplo, Instagram) a fin de establecer un contacto electrónico, generar confianza (quizás mandado imágenes también falsas o editadas), a fin de conseguir mayor información de la persona investigada, como localidad donde se encuentra, barrio donde vive, etc.



2.2.5. Registro Remoto

2.2.5.1. ¿En qué consiste?

- Consiste en una medida que autoriza, en el marco de una investigación de un delito de gravedad, siempre que no existe otra medida menos invasiva de la privacidad, la realización de un acceso de forma remota y sin el conocimiento del titular o usuario del dispositivo o sistema que es objeto de investigación, mediante la utilización de programas informáticos u otros mecanismos tecnológicos, a fin de poder acceder y recolectar datos informáticos que sean de utilidad para probar el delito investigado, o incluso, determinar al autor/a del mismo.

2.2.5.2. ¿Quién puede solicitar la medida?

La respuesta depende de lo establecido normativamente por cada jurisdicción, pero por lo general y de acuerdo a nuestro estudio de derecho comparado internacional, se considera que para esta medida o técnica especial de investigación:

- Requiere de autorización judicial, toda vez que la ejecución de la medida implica un nivel alto de injerencia s los derechos de la o las personas afectadas, ya que implica ocultar la verdadera identidad del agente, simular otra identidad, hasta incluso, el envío o compra de material ilícito, todo con la finalidad de conseguir ingresar en un ámbito de confianza de la banda.

- El o la Fiscal a cargo de la investigación debe enviar la solicitud al Juez o Jueza de Garantías (o que corresponda de acuerdo a la jurisdicción) a fin de que autorice la posibilidad de utilización de esta figura. La ejecución práctica de esta figura, generalmente es delegada a una fuerza de seguridad especializada, que debe permanecer siempre bajo el control de la Unidad Fiscal solicitante.

2.2.5.3. ¿Qué límites deberían especificarse en la orden?

- La descripción del hecho objeto de investigación y la identidad del investigado o de cualquier otro afectado por la medida, siempre que tales datos resulten conocidos.
- La orden judicial que autorice la medida deberá fundamentar su necesidad, razonabilidad y proporcionalidad (establecidos en la sección 1.3 de la presente Guía o en caso de existir, en el Código Procesal Local aplicable), justificando especialmente la ponderación de su utilidad con relación a la afectación de derechos fundamentales involucrados, la gravedad del hecho investigado y que no existen medios menos intrusivos de la intimidad del imputado que resulten útiles para alcanzar los mismos fines probatorios.
- En el caso de ser posible, deberá designarse el o los dispositivos o conexiones que serán objeto de la medida.
- En el caso de ser posible, deberá designarse la tecnología, técnica o software especializado que se utilizará para intentar la medida.
- Deberá ordenarse el control de la medida, por parte de la Fiscalía a cargo, de registrar toda la información necesaria respecto a los avances de la medida, priorizando en todo momento garantizar la integridad y confidencialidad de la información.
- En los casos donde se considere necesario, el Juez de Garantías podrá autorizar que, una vez realizado el ingreso, se puedan adoptar medidas técnicas que permitan lograr que el mismo sea permanente (por ejemplo, modificando o deshabilitando ciertas restricciones del sistema objetivo).
- La medida será autorizada por el plazo estrictamente necesario para lograr la individualización de los autores, partícipes o encubridores, o para obtener y asegurar los medios de prueba necesarios para su prosecución.

2.2.5.4. Notas adicionales

- Considerar que en la actualidad, conseguir acceso subrepticio a un sistema informático, es una tarea que a menos que se cuente con software especializado, realizarlo o intentarlo de forma artesanal puede ser de mucha complejidad. Advertimos esto, porque puede suceder que al momento de realizar esta solicitud, aún no se tenga conocimiento concreto del sistema objeto de la medida (por ejemplo, si posee un sistema operativo Windows, o es un dispositivo celular con Android). Advertimos esto, toda vez que si bien es deseable que al momento de la solicitud de la medida se tenga el mayor nivel de certeza posible, a fin de garantizar los límites y bordes de la medida autorizada, en muchos casos, puede no ser posible.
- En caso de ser posible, y con la finalidad de tener mayores probabilidades de éxito en la medida intentada, se sugiere que la Fuerza de Seguridad dedicada a la ejecución de este tipo de medidas, tenga previamente generado protocolos o técnicas de ejecución de las medidas de acuerdo al tipo de sistema operativo o dispositivo objetivo.

2.2.5.5. ¿Qué obtendría de esta solicitud?

- La autorización para intentar el acceso subrepticio al sistema o dispositivo utilizado por la o las personas sospechadas, que nos permita obtener información de interés para el delito investigado.

2.2.5.6. Un ejemplo concreto del uso de esta medida o técnica especial de investigación

- Ante el caso de una investigación por un caso de distribución de material de abuso sexual infantil, donde se tiene información acerca que el sospechoso utiliza distintas técnicas anti forenses para evitar ser perseguido y acusado (por ejemplo, utiliza conexiones a través de TOR, o posee un sistema de cifrado en el equipo que incluso teniendo un allanamiento, no será posible el acceso a la información de la misma). Habiéndose intentado otras técnicas o medidas de investigación sin éxito, podría solicitarse este tipo de medida, a fin de autorizar a un agente de una fuerza de seguridad a intentar el acceso subrepticio a los sistemas o dispositivos de la persona sospechada. En el caso que sea técnicamente posible, el agente podrá infiltrarse en su equipo, recolectando información de interés (como la verdadera ubicación de la persona, archivos que lograrían probar el delito, comunicaciones con otras personas relacionadas en el delito, etc.)

3.0. Del sistema de generación de modelos de escritos de órdenes o solicitudes de medidas o técnicas especiales de investigación

3.1. Advertencias legales

- El presente sistema o los escritos generados por el mismo, no deben ser considerados bajo ningún punto de vista como un asesoramiento profesional para el usuario, pensado para el uso interno de Ministerios Públicos Fiscales, así como Fuerzas de Seguridad vinculadas a la investigación del ciberdelito.
- El sistema no garantiza la exactitud de los resultados en relación a sobre si la medida o técnica especial de investigación solicitada puede o no pedirse en la jurisdicción a la que pertenece el usuario, ni si su sistema normativo permite o no la ejecución de la misma.
- El objetivo de la "Guía de Buenas Prácticas para la solicitud de Medidas o Técnicas Especiales de Investigación para casos de Cibercrimen" es fomentar la realización de pedidos de medidas de investigación, que tengan un mayor nivel de respeto y

compromiso por los derechos fundamentales, estimulando la práctica de fundamentar las medidas de acuerdo a su necesidad, razonabilidad y proporcionalidad.

3.2. Protección de Datos Personales

- Los datos personales recolectados no tienen ningún tipo de fin comercial. La única finalidad de la solicitud de los datos personales, en la propia generación del escrito y la posibilidad que el sistema pueda enviarle el modelo a su casilla de mail, toda vez que de momento no tenemos alternativa para poder brindarle el acceso al mismo. Los datos cargados no serán transferidos por ninguna razón y en su caso, su utilización será realizada de forma anonimizada y estadística, a fin de poder determinar, por ejemplo, que medida es la más solicitada, o cuantos días de preservación se piden en una medida, etc.
- La DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES, órgano de control de la Ley Nº 25.326, tiene la atribución de atender las denuncias y reclamos que se interpongan con relación al incumplimiento de las normas sobre protección de datos personales.

3.3. Acceso al sistema informático de la Guía

A fin de que pueda ser testeado como corolario final de esta tesis de doctorado, el sistema actualmente se encuentra funcional en el siguiente link o código QR:

https://bit.ly/3TP8WJI

Bibliografía

- ADC, El (des)control democratico de los organismos de inteligencia en Argentina. Publicado en Enero 2015, Disponible en: https://adc.org.ar/wp-content/uploads/2019/06/004-el-descontrol-democratico-de-los-organismos-de-inteligencia-en-argentina-01-2015.pdf
- AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD); "Estudio Fingerprinting o Huella digital del dispositivo", Disponible en: https://www.aepd.es/documento/estudio-fingerprinting-huella-digital.pdf
- ALLER, Germán. "Cuestiones Victimológicas de Actualidad: Origen de la Victimología, Seguridad, Cifra Negra, Personalización del Conflicto y Proceso Penal". Revista ILANUD Nro. 27, 2006.
- ANDERSON, Ross. "Security engineering: a guide to building dependable distributed systems". Editorial Wiley, ISBN 978-0-470-06852-6.
- BACIGALUPO, Enrique. "Manual de Derecho Penal". Editorial Temis. 1996, pág. 101
- BLANCO, Hernán, Tecnología Informática e investigación criminal, Ciudad Autónoma de Buenos Aires,La Ley, 2020, pág. 103. Con cita de Bellovin, Steven M. – Blaze, Matt – Clark, Sandy – Landau, Susan, "Going bright: Wiretapping without weakening communications infraestrcuture", en IEEE Security & Privacy, vol. 11, Nro. 1, 2013, Págs. 62/72.
- BOBBIO, Norberto. "Teoría General del Derecho"; 2da. Edición, Editorial Temis, 1994.
- BORGHELLO, Cristian Fabian, Tesis "Seguridad Informática. Su Implicancia e Implementación"- 2001, Reg.UTN/Facultad 0015/793
- BRENNER, S.W., 2004. Cybercrime Metrics: Old Wine, New Bottles? Virginia Journal of Law & Technology, 9(13):1-52. El delito cibernético también está incluido como ejemplo de un tipo de 'delito emergente y difícil de medir' en documentos de la 42a Sesión de la Comisión Estadística de las Naciones Unidas. Ver Consejo Económico y Social de las Naciones Unidas, Comisión Estadística, 2012. Informe del Instituto Nacional de Estadística y Geografía de México sobre Estadísticas Delictivas. E/CN.3/2012/3, 6 de diciembre de 2011.
- BRUZZONE, Gustavo, "La nulla coactio sine lege como pauta de trabajo en el proceso penal", Estudios sobre Justicia Penal. Homenaje al Profesor Julio B. J. Maier. Ed. Del Puerto, Bs. As. 2005.
- BUSANICHE, Beatriz; "El delito que cometemos todos", Fundación Via Libre. 2011. Url: http://www.vialibre.org.ar/2011/05/15/el-delito-que-cometemos-todos/
- CAFFERATA NORES, José I. y Hairabedian, Maximiliano, La Prueba en el Proceso Penal. Con especial referencia a los Códigos Procesales Penales de la Nación y de la Provincia de Córdoba, Sexta edición, Lexis Nexis, Argentina, 2008.

- CALVO LOPEZ, David, “Capacidades de actuación del Ministerio Público Fiscal y la Policía Judicial tras la reforma procesal operada por la Ley Orgánica 13/2015”, Jornadas de Especialistas celebradas en el Centro de Estudios Jurídicos de Madrid, 16 y 17 de Febrero de 2017. Url: https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/Ponencia%20Calvo%20L%C3%B3pez,%20David%20(2017).pdf?idFile=07e530e0-5ce6-4103-94f5-43a183c3e581
- CARRIÓ; Alejandro; “Garantías constitucionales en el Proceso Penal”, 5 edición actualizada y 119 ampliada, Editorial Hammurabi, Buenos Aires, 2008, pág. 353 y ss.
- CHALES, Juan Pablo; “Las técnicas de investigación penal a la luz del Convenio sobre ciberdelito y su aplicación en Argentina”, Tesis de Maestría, 2018. Universidad Nacional de Cuyo.
- CIANCIARDO, Juan, “El conflictivismo en los derechos fundamentales”, Eunsa, Pamplona, 2000, págin. 287-288
- CREUS, Carlos, "Derecho Penal: Parte General", 5ta. Edición actualizada y ampliada. Editorial Astrea. 2010
- DAVARA RODRIGUEZ, Miguel Ángel, Manual de Derecho Informático, Thomson Aranzadi, 10º edición, pág. 358 y 359.
- DEPARTAMENTO DE JUSTICIA DE LOS ESTADOS UNIDOS; Buró Federal de Investigaciones. 2000. National Incident-Based Reporting System. Volume 1: Data Collection Guidelines. Disponible en: http://www.fbi.gov/about-us/cjis/ucr/ucr
- DI IORIO, Ana Haydée …, “El rastro digital del delito : aspectos técnicos, legales y estratégicos de la informática forense”,1a ed . - Mar del Plata : Universidad FASTA, 2017
- DONNA, Edgardo y FUENTE, Esteban Javier. “Aspectos generales del tipo penal de estafa”, Revista de Derecho Penal, N° 2000-2, Rubinzal-Culzoni, p. 57
- DUPUY, Daniela; “Desafíos procesales en la investigación de delitos informáticos”, Libro: Informática y Delito: Reunión preparatoria del XIX Congreso Internacional de la Asociación Internacional de Derecho Penal (AIDP).
- ECKERSLEY, Peter,, “How Unique Is Your Web Browser?”, Electronic Frontier Foundation. Url: https://panopticlick.eff.org/static/browser-uniqueness.pdf
- ELECTRONIC FRONTIER FOUNDATION (EFF); Proyecto “Panopticlick”. Disponible en Url: https://panopticlick.eff.org/about#browser-fingerprinting
- ELECTRONIC PRIVACY INFORMATION CENTER (EPIC); Apple vs. FBI; Disponible en: https://epic.org/documents/apple-v-fbi-2/
- ENGLEHARDT, Steven y NARAYANAN, Arvind, “Online Tracking: A 1-million-site Measurement and Analysis”, Princeton University, Disponible en: https://dl.acm.org/doi/pdf/10.1145/2976749.2978313

- EUROPEAN DATA PROTECTION BOARD, Legado: Grupo de Trabajo del art. 29; Disponible en: https://edpb.europa.eu/our-work-tools/article-29-working-party_es
- FAFINSKI, S., Dutton, W.H. and Margetts, H., 2010. Mapping and Measuring Cybercrime. Oxford Internet Institute Forum Discussion Paper No. 18., Junio de 2010.
- FERNANDEZ DELPECH, Horacio, Manual de Derecho Informático, 1ra. Edición, Ed. Abeledo Perrot, Argentina, 2014, Pág. 194
- FERRAJOLI, Luigi; Derecho y Razón. Teoría del garantismo penal (Madrid: Editorial Trotta, 1995), 610.
- FUERTES-PLANAS ALEIX, Cristina; "Validez, obligatoriedad y eficacia del derecho en H. L. A. Hart", Anuario de Derechos Humanos. Nueva Época. Vol. 8. 2007 (131-186). España.
- FUMIS, Federico, "La utilización de modernas tecnologías en la persecución penal: su utilidad en la búsqueda de mayores índices", publicado en REDI: Revista Electrónica de Derecho Informático. Número 44
- FUNDACIÓN VÍA LIBRE: "Comunicado: organizaciones de derechos humanos rechazan medidas arbitrarias contra el investigador en seguridad digital Javier Smaldone"; Disponible en: https://www.vialibre.org.ar/comunicado-organizaciones-de-derechos-humanos-rechazan-medidas-arbitrarias-contra-el-investigador-en-seguridad-digital-javier-smaldone/
- KRANZBERG, Melvin; "Technology and Culture", Vol. 27, No. 3 (Jul., 1986), pp. 544-560
- GARCÍA, Luis, "La intervención de las comunicaciones telefónicas y otras telecomunicaciones en el Código Procesal Penal de la Nación: un cheque en blanco para espiar nuestra vida privada", publicado en Cuadernos de Doctrina y Jurisprudencia Penal, nro. 6, 1997, editorial Ad Hoc, Buenos Aires.
- GARIBALDI, Gustavo, Tesis Doctoral Las Modernas Tecnologías de Control y de Investigación del delito. Su incidencia en el derecho penal y los principios constitucionales, editorial Ah Hoc, 2010.
- GERCKE, Marco, Understanding Cybercrime. Phenomena, Challenges and Legal Response, publicación del Cybercrime Research Institute, segunda edición, agosto del 2011. International Telecommunication Union, Manual de Comprensión del Ciberdelito. Fenómenos, Dificultades y Respuestas Jurídicas, publicación de la versión en Español de Septiembre del año 2012, disponible en http:// www.itu.int/en/ITU-D/Cybersecurity/Pages/Legal-Measures.aspx
- GOLDSMITH, Jack, "The internet and the Legitimacy of Remote Cross Border Searches", publicado en Public Law And Legal Theory Working Paper nro. 16, The Law School, University of Chicago, 2001.
- GONZÁLEZ PÉREZ, J. J. Utilización en el proceso penal de datos vinculados a las comunicaciones electrónicas recopilados sin indicios de comisión delictiva en "Protección de datos y proceso penal". Ed. La Ley, 2010, pág. 356

- HERRERA BRAVO, Rodolfo. “El Derecho en la Sociedad de la Información: Nociones generales sobre el Derecho de las Tecnologías de la Información y las Comunicaciones.”, Publicado en DerechoTecnologico.com, Url: http://www.derechotecnologico.com/estrado/estrado002.html
- HIMMANEN, Pekka. “La ética hacker y el espíritu en la era de la información”. Edición Digital de Licencia GPL. Url: http://www.educacionenvalores.org/IMG/pdf/pekka.pdf
- INFO-LAB; “Guía integral de empleo de la informática forense en el proceso penal”; Url: https://www.pensamientopenal.com.ar/system/files/2019/02/doctrina47360.pdf
- JIJENA LEIVA, Renato Javier: “La Criminalidad Informática”: Situación de Lege Data y Lege Ferenda en Chile”. Actas de III Congreso Iberoamericano de Informática y Derecho”. Mérida, España.
- JIMÉNEZ DE ASÚA; “Tratado de Derecho Penal”,Editorial Losada; ps. 388 y siguientes
- KELSEN, Hans; Bulygin, Eugenio. "Validez y eficacia del Derecho". Ed. ASTREA, 2005.
- KERR O, “Computer Crime Law”, 3º Ed., 2013, p. 532.
- KERR-SCHNEIER; Encryption Workarounas, en “Georgetown Law Journal”, vol. 106, n*4, 2018, ps. 994 y ss. y 1003 y siguientes.
- KERR, O; Compelled Decryption and the Privilege Against Self-Incrimination, en “Texas Law Review”, vol 97, Nº4, 2019.
- KERR, O; Executing warrants for digital evidence: the case for use restrictions on nonresponsive data, en “Texas Tech Law Review”, vol. 48, n* 1, 2015, p.21 y siguientes.
- KERR, O, Digital Evidence and the New Criminal Procedure. 105 Columbia Law Review 279 (2005), Disponible en SSRN: https://ssrn.com/abstract=594101
- MAIER, Julio; Derecho Procesal Penal. Tomo I, pág. 681
- MINISTERIO DE SEGURIDAD DE LA REPÚBLICA ARGENTINA, Resolución 144/2020: “Protocolo General para la prevención policial del delito con uso de fuentes digitales abiertas”; Disponible en: https://www.boletinoficial.gob.ar/detalleAviso/primera/230060/20200602
- MIR PUIG, Santiago; “Introducción a las bases del derecho penal: Concepto y Método”, Editorial BdF, 2003
- MOSHIRNIA, Andrew:, “Separating hard fact from hard drive: a solution for plain view doctrine in the digital domain”, en “Harvard Journal of Law 8. Technology”, vol. 23, n*2, 2010, ps. 611 y 612
- MOWERY, Keaton y SHACHAM, Hovav; “Pixel Perfect: Fingerprinting Canvas in HTML5”, Departamento de Ingeniería y Ciencias de la Computación de la

Universidad de San Diego, California, EEUU; Disponible en: https://hovav.net/ucsd/dist/canvas.pdf

- NACIONES UNIDAS, "Estudio exhaustivo sobre el delito cibernético", 2013, Url: https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime_Study_Spanish.pdf
- NACIONES UNIDAS, Asamblea General, "Lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos", 2019, Disponible en: https://www.unodc.org/documents/Cybercrime/SG_report/V1908185_S.pdf
- NEME, Catalina F., "Una mirada actual en materia de regulación de retención de datos de tráfico y conservación rápida de datos informáticos" en DUPUY Daniela y KIEFER Mariana, "Cibercrimen" Editorial BdeF, Buenos Aires, 2017
- NINO, Carlos; Fundamentos de Derecho constitucional, pág. 304
- ORGANIZACIÓN DE ESTADOS AMERICANOS (OEA); AG/RES. 2004 (XXXIV-O/04), Año 2004
- ORTIZ PRADILLO, Juan Carlos, "La investigación del delito en la era digital: Los derechos fundamentales frente a las nuevas medidas tecnológicas de investigación". Estudios de Progreso – Fundación Alternatives, Url: http://www.falternativas.net/public/storage/actividades_descargas/b78e188fdcae153bcd14b71e5ca618e7.pdf
- PALAZZI, Pablo Andrés, "Delitos Informáticos", Ad-Hoc, Buenos Aires, 2000.
- PALAZZI, Pablo. Los delitos informáticos en el Código Penal. Análisis de la ley, Editorial Abeledo & Perrot, A. (2016).
- PANTOJA RUIZ, Juan Pablo; "BSBD por la defensa en el proceso penal"; Disponible en: https://www.asuntoslegales.com.co/consultorio/bsbd-por-la-defensa-en-el-proceso-penal-3418941
- PECES-BARBA, Gregorio; FERNANDEZ, Eusebio; DE ASIS, Agustin; "Curso de Teoría del Derecho". Ed. Marcial Pons, 1999, Madrid.
- PÉREZ BARBERÁ, Gabriel, El Principio General de Reserva de Ley (o principio general de legalidad en la doctrina alemana); Nuevas Tecnologías y libertad probatoria en el proceso penal, ponencia presentada en el VI Encuentro Nacional de Profesores de Derecho Procesal Penal, Salta, mayo de 2009.
- PERRON, Walter, "Perspectivas de la unificación del derecho penal y del derecho procesal en el marco de la Unión Europea", en AAVV, Estudios sobre Justicia Penal. Homenaje al Profesor Julio B. J. Maier, Bs. As., Editores del Puerto, 2005, pp. 734/735 y 737/738.
- POLANSKY, Jonathan, "Garantías constitucionales del procedimiento penal en el entorno digital"; 1º Edición, Editorial Hammurabi. 2020

- QUEIROZ, Jordan y FEITOSA, Eduardo, "A Web Browser Fingerprinting Method Based on the Web Audio API", The Computer Journal, Volume 62, Issue 8, August 2019, Pages 1106–1120, Disponible en: https://doi.org/10.1093/comjnl/bxy146
- RIQUERT, Marcelo Alfredo, "Estado de la Legislación contra la Delincuencia Informática en el Mercosur" (en línea), URL: http://www.pensamientopenal.com.ar/node/ 27142
- RIQUERT, Marcelo: "Convenio sobre Cibercriminalidad de Budapest y el Mercosur Propuestas de derecho penal material y su armonización con la legislación regional sudamericana", Publicado en Revista Derecho Penal. Año III, N° 7 pág. 107, Infojus, Id SAIJ: DACF140393
- RODRÍGUEZ CARO, María Victoria. "La infiltración policial: en el límite del Estado de Derecho. El inminente agente encubierto informático"; Editorial Academica Espanola (8 Junio 2015)
- SALT, Marcos, "Nuevos Desafíos de la evidencia digital. El Acceso transfronterizo de datos en los países de América Latina", publicado en Derecho Penal y Procesal Penal, editorial Abeledo Perrot, Buenos Aires, 2013;
- SALT, Marcos, Criminal Procedure Law Provisions on Cybercrime in Latin America Regarding Their Compliance with the Budapest Convention (Argentina, Chile, Colombia, Costa Rica, Mexico, Paraguay and Peru), informe preparado para el consejo de Europa, Estrasburgo, 2011; Identity related crime in Latin American Countries, Estudio realizado para el Grupo de Expertos sobre Identidad Robada de Naciones Unidas (UNODC), diciembre del año 2010;
- SALT, Marcos, Prólogo en libro "Vigilancia electrónica y otros modernos medios de prueba", del Abog. Carlos Christian Sueiro, Ed. Hammurabi, 2017. Url: http://www.libreriahammurabi.com/prologos/PrologoSaltSueiro.pdf
- SALT, Marcos; "Nuevos Desafíos de la evidencia digital. El Acceso transfronterizo de datos en los países de América Latina". Disponible en: https://aadproc.org.ar/pdfs/biblioteca_virtual/Congreso_2015/Ponencias%20Generales/Procesal%20Penal/SALT%2C%20Marcos.pdf
- SALT, Marcos; Prólogo del Libro "Vigilancia electrónica y otros modernos medios de prueba", de Sueiro Carlos Christian, 2019, 2da. edición.
- SEGU-INFO; "Wannacry: al menos 75 países afectados", URL: http://blog.segu-info.com.ar/2017/05/wannacrypt-al-menos-15-paises-afectados.html
- SIEBER, Ulrich, The International Handbook on computer Crime, Ed. John Wiley &sonsUd, 1986, Gran Bretaña.
- SILVA SANCHEZ, Jose María, "La expansión del derecho penal. Aspectos de la política criminal en las sociedades postindustriales. Editorial B de f, Montevideo – Buenos Aires. 2011

- STRATIOTIS, Diego: “Los allanamientos remotos y el uso de drones o robots”, Disponible en: https://jusmendoza.gob.ar/wp-content/uploads/2022/06/Stratiotis-Diego.pdf
- TARUFFO, Michele, “Algunas consideraciones sobre la relación entre prueba y verdad”, en La prueba. Artículos y conferencias (Santiago: Metropolitana 2008), 59-66.
- TARUFFO, Michelle: “Simplemente la verdad: el juez y la construcción de los hechos”; Madrid. Marcial Pons, 2010, Pág. 115.
- TÉLLEZ VALDÉS, Julio, "Derecho Informático", 3ª.ed., Ed. Mc Graw Hill, México, 2003, Pág. 8
- TEMPERINI, Marcelo y BORGHELLO, Cristian, “Suplantación de Identidad Digital como delito informático”. Doctrina publicada en el Libro “Cibercrimen: aspectos de Derecho penal y procesal penal. Cooperación internacional. Recolección de evidencia digital. Responsabilidad de los proveedores de servicios de internet”. Directora: Daniela Dupuy. ISBN: 9789974745063; Editorial: Editorial B de f; 2016.
- TEMPERINI, Marcelo y MACEDO Maximiliano; “OSINT: Legalidad y protección de datos personales”, publicado en el libro “Protección de datos. Doctrina y jurisprudencia - Tomo 2”, dirigido por Pablo Palazzi.
- TEMPERINI, Marcelo y MACEDO, Maximiliano, “Nuevas herramientas para la investigación penal: El agente encubierto digital”, Cibercrimen. Aspectos de derecho penal y procesal penal. Cooperación internacional. Recolección de evidencia digital. Responsabilidad de los proveedores de servicios de Internet. Editora: Daniela Dupuy. Editorial: BdeF, 2017.
- TEMPERINI, Marcelo; “Deep web, anonimato y Cibercrimen”. VI Congreso Iberoamericano de Investigadores y docentes de Derecho e Informática (CIIDDI 2016). ISBN: 9789876921381, 2016.
- TEMPERINI, Marcelo; Delitos informáticos y cibercrimen; Técnicas y tendencias de investigación penal y su afectación a los derechos constitucionales; Cibercrimen II. Nuevas conductas penales y contravencionales. Inteligencia artificial aplicada al Derecho penal y procesal penal. Novedosos medios probatorios para recolectar evidencia digital. Cooperación internacional y victimología. Directora y Coordinadoras: Dupuy, Daniela - Kiefer, Mariana y otros. Año 2018. Edición 1ª
- TREND Micro; “Tendencias en la seguridad cibernética en América Latina y el Caribe y respuestas de los gobiernos”, 2013, Secretaría de Seguridad Multidimensional de la OEA. ISBN 978-0-8270-6061-6
- VANINETTI, Hugo “Agente encubierto y la pornografía infantil en internet”, publicado en LA LEY, DJ 02/11/2011, Cita Online: AR/DOC/2722/2011
- VAZQUEZ SECO, Luis, “Retención obligatoria de datos de tráfico de las comunicaciones telefónicas y/o electrónicas. análisis de la sentencia del tribunal de

justicia de la unión europea de 8 de abril de 2014 en los asuntos acumulados c-293/12 y c594/12 (Digital Rights Ireland y Seitlinger y otros)

- VELASCO, Núñez, E.: Delitos tecnológicos: definición, investigación y prueba en el proceso penal, Madrid, 2016, p. 68
- WELZEL, ZStW, 58, §. 491 ss., 509, cit. por JAKOBS, Günther, Derecho penal. Parte general. Fundamentos y teoría de la imputación, 2ª ed., trad. de Joaquín Cuello Contreras y José Serrano González de Murillo, Marcial Pons, Madrid, 1997 [2ª ed. alemana 1991], ps. 47 y 48