UNIVERSIDAD NACIONAL DEL LITORAL - FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES

SECRETARÍA DE POSGRADO

ESPECIALIZACIÓN EN DERECHO ADMINISTRATIVO FCJS|UNL.

COHORTE 2021

Sede ENTRE RÍOS

LIMITES AL TRATAMIENTO DE DATOS PERSONALES

El rol del Estado entrerriano frente al acceso, tratamiento y divulgación de los datos personales recabados por la Administración Pública local

Director: Dr. Federico Lacava

Alumna: Victoria Inés Aizicovich

PARANA, 2024.

V. <u>INDICE</u>

TITULO: LIMITES AL TRATAMIENTO DE DATOS PERSONALES. El rol del Estado entrerriano frente al acceso, tratamiento y divulgación de los datos personales recabados por la Administración Pública local

LIMITES AL TRATAMIENTO DE DATOS PERSONALES.

El rol del Estado entrerriano frente al acceso, tratamiento y divulgación de los datos personales recabados por la Administración Pública local.

SUMARIO.

Se busca explorar, a través de un estudio básico y documental, sincrónico y microsocial, el rol de la Administración Pública local frente al debido acceso, tratamiento y manipuleo de los datos personales recabados por el Estado provincial; como así también la vigencia de un ordenamiento administrativo y de contralor en consonancia con el sistema jurídico administrativo internacional compuesto por diversas fuentes de aplicación transversal, ello con el eje centrado en la persona humana y su dignidad, como así también en torno a la garantía de los derechos humanos a la vida privada, dignidad y autodeterminación informativa, analizando -con ello- los nuevos desafíos de la Sociedad Digital.

En efecto, se impetra plasmar el actual desafío que implica para la Administración local, máxime para los emergentes gobiernos electrónicos, el correcto manipuleo de los datos personales a los que se tiene acceso y, consecuentemente, la gestión y debido uso de la información, considerando que los nacientes procesos de digitalización de los registros públicos y ordenamiento de base de datos reclaman una asertiva regulación direccionada a la protección de los derechos fundamentales, con mas que, actualmente, los límites al tratamiento de los datos personales por parte del Estado local se evidencian difusos, poco claros, discrecionales y, sin duda, desconocidos por el ciudadano de a pie e incluso por operadores estatales; todo lo cual abre la puerta a un uso irrestricto y deliberado de la información.

PALABRAS CLAVE:

Datos Personales. Autodeterminación Informativa. Sociedad Digital. Organización Administrativa. *SoftLaw*. *Big Data*. Nativos Digitales. Estado Digital. Administración Pública global.

I.- PROBLEMÁTICA. CONSTRUCCION DEL OBJETO. RELEVANCIA

El presente trabajo busca indagar acerca de los límites existentes, en el campo de la Administración Pública entrerriana, al acceso, tratamiento y divulgación de los datos protegidos por la Ley de Protección de Datos Personales, cuya guarda surge como manda del Estado, como así también la relación entre los organismos que detentan el dato, los pretensores, tanto del sector público como del sector privado, y la ciudadanía, explorando los desafíos organizacionales, procedimentales y normativos para un correcto y asertivo método que considere los nuevos procesos de digitalización, almacenamiento de datos y acceso a la información.

Ciertamente, el estudio realizado se focalizó en la debida gestión y uso de la información a la que accede la Administración local, considerando que los nacientes procesos de digitalización y ordenamiento de base de datos reclaman una organización reglada para evitar cruzar los límites que impone la normativa imperante, máxime en tanto se evidencia un uso discrecional y deliberado de la información por parte del Estado.

Sobre el particular, y previo adentrarme al análisis concreto del objeto, considero pertinente referenciar que el disparador del análisis realizado fue producto de haber abordado la temática -para mi novedosa- de la organización y procedimiento interno de la Administración desde una óptica metodológica, esto es vinculado a los Módulos III "La Organización Administrativa y la Gestión Pública" y IX "Derecho Internacional y Derecho Administrativo" de la carrera cursada; en las que -entre otras-, se puntualizó en la imperiosa necesidad de contar con una organización reglada dentro de todo estamento para la consecución de los fines, de la estrecha relación con una necesaria reglamentación que conduzca a los operadores y agentes a un fin común y a la obtención de resultados óptimos, como así también a la vinculación que dicha reglamentación debe tener con el derecho administrativo internacional, considerando a todo evento la multiplicidad de fuentes de derecho administrativo.

En efecto, la metodología de organización interna de las Administraciones Púbicas reclama como punto de partida normas y principios de derecho que orienten el mejor mecanismo para resguardar y tutelar derechos en la consecución de los fines; los cuales -en los tiempos que corren- no pueden escindirse del derecho internacional aplicado al ámbito local. La vinculación es mandatoria, la búsqueda en los principios generales y en el *SoftLaw* internacional sobreviene cada vez con mayor peso en la toma de decisiones y ello, sin duda alguna, refuerza la necesidad de adecuarse a un ámbito de administración transfronterizo que reclama atender y entender a la Administración como un conjunto de procedimientos afines, precedidos por una organización reglada que no puede ser dejada al arbitrio de los usos y costumbres locales.

Ello así, se reitera, el presente trabajo, con sustento en los conceptos incorporados en el desarrollo del curso, y en especial en los módulos referenciados, impetra por indagar dichos procesos internos vinculados a la tutela de los datos personales, en el ámbito local, su tratamiento y debido uso, para determinar si los mismos -de existir- se corresponden a los parámetros normativos vigentes, nacionales e internacionales que abordan la temática y, en su caso, proponer soluciones o alternativas viables para concretizar una oportuna regulación al efecto.

Históricamente, los registros públicos que receptan datos personales detentan un mecanismo de recopilación y archivo de la información que les permite el manipuleo discrecional del dato conforme los parámetros de la ley de protección de datos personales (interés legítimo y derecho subjetivo), ello mediante su otorgamiento al particular u a otros organismos estatales o privados a través de la conformación de convenios de colaboración, gratuitos u onerosos, que detenten un fin de interés público, esto último también discrecional.

En otras palabras, al ingresar el dato a la órbita estatal, dicha información es gestionada por el Estado, lo que implica una mayor exigencia o responsabilidades sobre su estructura organizativa, teniendo en miras cada uno de los aspectos implicados en esa gestión (registro, almacenamiento, accesibilidad, seguridad, utilización para “fines públicos”).

Ciertamente, los avances tecnológicos en las formas de registrar y almacenar información pero, sobre todo, en los mecanismos de tratamiento y divulgación, acarrean un conjunto de oportunidades beneficiosas y asimismo de efectos consecuenciales, cuyo

análisis demanda una comprensión global de los impactos de la digitalización en la vida social.

Los sistemas de información generados como soportes para la gestión de políticas públicas y toma de decisiones, en particular en el campo de la protección de los derechos sociales, se presentan como una de las dimensiones institucionales prioritarias en la era contemporánea y, correlativamente, demandan un mayor y más cauteloso análisis.

Hoy en día, con la informatización y digitalización del dato, surgen como obsoletos los mecanismos de protección, por cuanto la evolución social y tecnológica genera nuevos medios y procedimientos para la difusión y gestión de la información lo que, en conjunción con la inteligencia artificial, plantea genuinos retos para la protección de la privacidad, e interpela a la elaboración de herramientas efectivas que doten a la Administración Pública de la potestad de guardiana y tutora de la información, y de un correcto uso de tamaña materia prima.

Frente a tal escenario de situación resulta relevante la necesidad de indagar acerca de la efectiva gestión de la información en la era digital y, asimismo, el correcto tratamiento de los datos personales que la Administración debe endilgar, en procura de la protección *per se* de los derechos fundamentales en juego; máxime atendiendo a que, en la mayoría de los casos, cuando los ciudadanos o personas de existencia ideal aportan información a las bases de datos, desconocen los límites y los alcances que tendrán y con qué fines podrán ser utilizados.

A decir de Pérez Hualde, actualmente la actividad administrativa se encuentra reglada sobre nuevas bases de derecho administrativo constitucional, el cual aspira a la realización de los derechos sociales fundamentales, siendo la dignidad de la persona humana el fundamento del orden político y la paz social, que impetra a un interés general.

Deviene innegable, asimismo, que la correcta utilización de la información y el fácil acceso a su masividad y recopilación genera múltiples beneficios en la actualidad, sobre todo en lo que respecta a la generación y puesta en marcha de políticas públicas concretas relacionadas con el bienestar y la calidad de vida; ahorrando tiempo, dispendio económico y de recursos humanos, siendo que la información se encuentra a un *click* de distancia.

Sin perjuicio de ello es un deber, como correlato, reglamentar en debida forma el tratamiento y uso de esa información por parte del Estado y, consecuentemente, el conocimiento que la sociedad detenta acerca de cómo impactará en su vida cotidiana ese acceso. Ello reclama un pormenorizado estudio de la necesaria relación entre el dato, su tratamiento por parte de la Administración y divulgación a terceros o, incluso, dentro del propio Estado.

Surge manifiesto que el valor del dato radica en su propia definición, como materia prima para generar información con valor agregado, por lo que el análisis debe centrarse asimismo en el concepto que la Administración adopta acerca de "dato personal"; el alcance del "interés público" como habilitante de su tratamiento sin limitaciones, y demás elementos que delimiten el alcance de la materia frente a la subjetividad de quien la manipula, ello con el objeto de brindar una protección significativa.

En ese sentido, resulta dable referenciar que el concepto de "datos sensibles" ha sido redefinido recientemente por la Organización de los Estados Americanos en el 86° período ordinario de sesiones desarrollado en Río de Janeiro Brasil el 23-27 de marzo de 2015 (Informe del Comité Jurídico Interamericano, 2015).[1] Lo cierto es que resulta ser una noción que depende de su contexto, un dato no es sensible *per se* pero su uso puede derivar en discriminación afectando el derecho a la igualdad reconocido como un derecho humano, especificado en nuestra Carta Magna en el art 16. Es por ello que merecen un mayor nivel de protección.

El citado informe del Comité Jurídico Interamericano explica: "La frase "datos personales sensibles" se refiere a una categoría más estrecha que abarca los datos que afectan a los aspectos más íntimos de las personas físicas. Según el contexto cultural, social o político, esta categoría podría abarcar, por ejemplo, datos relacionados con la salud personal, las preferencias sexuales, las creencias religiosas o el origen racial o étnico. En ciertas circunstancias podría considerarse que estos datos merecen protección especial porque, si se manejan o divulgan de manera indebida, podrían conducir a graves perjuicios para la persona o a discriminación ilegítima o arbitraria".

Como consecuencia, es menester indicar que no hay una categoría específica a la que podamos identificar como dato personal sensible en sí. La doctrina entiende que un dato

[1] https://www.redipd.org/sites/default/files/inline-files/Informe_CJI-doc_474-15_rev2_26_03_15.pdf

ordinario puede convertirse en un dato sensible por su uso o tratamiento discriminatorio "(…) ejemplo muy sencillo: registrar el dato referido a la calidad de fumadora o no de una persona a los fines de destinarle ubicación en un restaurante no es lo mismo que hacerlo en un registro de seguros de vida." (Travieso Juan Antonio, 2006). Es importante comprender que el concepto de "dato sensible" no es estático, sino que evoluciona en consonancia con las disímiles circunstancias sociales, culturales, de tiempo y lugar.

A los fines del presente trabajo se ha adoptado la definición brindada por el Reglamento Europeo (UE) 2016/679[2] en relación a "dato personal", que impetra por abarcar todas las realidades emergentes y las nuevas formas desarrolladas por la tecnología; a saber: "A efectos del presente Reglamento se entenderá por: 1) «datos personales»: toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona…".

Ciertamente, el concepto de dato personal se adapta a los nuevos tiempos, recogiendo incluso jurisprudencia del Tribunal de Justicia Europeo de los últimos años y, siguiendo lo dispuesto por el grupo de trabajo del Art. 29 en su Dictamen sobre concepto de datos personales[3]: "Si bien la identificación a través del nombre y apellido es en la práctica lo más habitual, esa información puede no ser necesaria en todos los casos para identificar a una persona. Así puede suceder cuando se utilizan otros «identificadores» para singularizar a alguien. Efectivamente, los ficheros informatizados de datos personales suelen asignar un identificador único a las personas registradas para evitar toda confusión entre dos personas incluidas en el fichero. También en Internet, las herramientas de control de tráfico permiten identificar con facilidad el comportamiento de una máquina y, por tanto, la del usuario que se encuentra detrás. Así pues, se unen las diferentes piezas que componen la personalidad del individuo con el fin de atribuirle determinadas decisiones. Sin ni siquiera solicitar el nombre y la dirección de la persona es posible incluirla en una categoría, sobre la base de criterios socioeconómicos, psicológicos, filosóficos o de otro tipo, y atribuirle determinadas decisiones puesto que el punto de contacto del individuo (un ordenador) hace innecesario conocer su identidad en sentido estricto. En otras palabras, la posibilidad de identificar a una persona ya no equivale necesariamente a la capacidad de poder llegar a conocer su nombre y apellidos…".

[2]Art. 4.1 del nuevo Reglamento: https://www.boe.es/doue/2016/119/L00001-00088.pdf

[3]Dictamen 4/2007 del Grupo de trabajo del artículo 29 sobre el concepto de datos personales, adoptado el 20 de junio de 2007, disponible en El Considerando 26 del Reglamento completa la definición del artículo 4.1.

Huelga cuestionarse, entonces, cuál es el alcance material de dicho concepto frente a la subjetividad de quien se lo plantea, ello con el objeto que su protección sea relevante y asequible en el plano reglamentario. Ello así, siguiendo idéntico lineamiento planteado en los Principios esbozados en el Informe citado *ut supra*, pues se reconoce que la "sensibilidad" de los Datos Personales puede variar según la cultura y cambiar con el tiempo, y que los riesgos de ocasionar daños reales a una persona como consecuencia de la divulgación de Datos podrían ser insignificantes en una situación en particular, pero podrían poner en peligro la vida en otra.

El concepto no es estático, sino dinámico; razón por la cual el Estado debiera posicionarse en una postura de tutela que contemple esa variabilidad e, incluso, el caso concreto.

Sin duda alguna, la protección de datos a nivel doméstico o interno se encuentra cada vez más atravesada por los principios y normas internacionales. Al reglamentar a nivel interno no puede desoírse que existe un Estado Constitucional de Derecho que, a través de su Carta Magna, ha adherido a los principios rectores en el plano global y que, directa o indirectamente, afectan la vida cotidiana de los individuos.

En efecto, el mundo apunta hacia un ciudadano global, porque el individuo ya no se comporta solamente en lo local, sino en un espacio administrativo difuso que no reconoce espacios específicos y determinados de actuación.

En ese sentido, tal como refieren Kingsbury, Krisch y Stewart[4] los avances tecnológicos generan la imperiosa necesidad de un flujo de datos que trascienden las fronteras y, asimismo, el tratamiento de los datos de acceso domestico por parte de la Administración local impacta directamente en lo trasnacional. La acción administrativa global influye en la reglamentación administrativa local, ambos despliegues se conectan, dialogan y se articulan constantemente.

En otras palabras, no podemos actuar solos, a nuestro antojo y en un manipuleo discrecional, si de datos se trata; sino siguiendo estándares establecidos como común denominador. Hoy en día, las transformaciones sociales, políticas y tecnológicas impetran

[4]BENEDICT KINGSBURY, NICO KRISCH Y RICHARD B. STEWART. El surgimiento del Derecho Administrativo Global.

una mutación de la administración pública que delimite el efectivo tratamiento de los datos para sus propios fines.

Sin ir más lejos, los datos obtenidos por la identificación biométrica[5] de los ciudadanos a través de la tramitación de los documentos de identidad o pasaportes, con sistemas centralizados de provisión de bienes y servicios públicos en diversas áreas y sacando provecho de dichas tecnologías -presentándose no solo como la principal campaña del derecho a la identidad, sino como la forma de cumplir un pre requisito tecnológico para compartir información-, unifica la entrada a distintos sistemas de información, facilitando la individualización de los usuarios, sus trayectorias, el seguimiento poblacional, control de recursos, entre otros. O, en su caso, la utilización de la robótica en la gestión de políticas públicas de CABA mediante el desarrollo pormenorizado de "BOTI", asistente virtual que genera vínculo directo con el ciudadano para evacuar dudas a través del chat box de WhatsApp que, asimismo, es utilizado para recopilar datos, recabar encuestas y medir el humor social.

Todo lo antedicho reclama -asimismo- un nuevo marco regulatorio que controle el acceso, el tratamiento y debido uso de los datos a los que se accede; máxime considerando que muchas veces las políticas públicas de la mano de la tecnología y la ciencia arremeten en la sociedad a una velocidad inalcanzable, que torna imposible arribar a la normativa adecuada, a tiempo, que se amalgame con la protección necesaria e inescindible de las prácticas mencionadas.

No puede desoírse que, toda la tecnología y cientificidad de punta puesta al servicio de la Administración para mejorar la calidad de vida y la relación Estado-ciudadano, surge marcadamente como una imposición progresiva que no acepta marcha atrás, y que genera implícitamente una diferenciación entre los ciudadanos que ingresan al sistema digital y los

[5]Datos Biométricos: Conjunto de tecnologías que miden y analizan datos de reconocimiento únicos que facilitan los procesos de verificación o autenticación y de identificación. La verificación o autenticación biométrica es una comparación uno a uno que permite validar la identidad de un individuo mediante la comparación de datos entre las características de un individuo con su plantilla biométrica existente, para determinar el parecido y crear un modelo de referencia que se guarda en un sistema de gestión de identidad o *template*, el que posteriormente permite la autenticación. En la mayoría de los casos, los datos personales, biométricos o sensibles son recolectados, analizados, almacenados, usados o compartidos con poco conocimiento y control de los individuos, lo que compromete la privacidad, seguridad y confianza. Estos datos pertenecen sin embargo a los individuos que identifican, son una extensión informacional de ellos relativa a su vida privada, pública y profesional y no deberían ser tratados como propiedad de una organización de ningún carácter, sino como un derecho que ya es reconocido en el artículo 8 de la Carta de los Derechos de la Unión Europea y por el artículo 16 del Tratado de Lisboa, por lo que debería ser reconocido y protegido a nivel mundial. Al ser únicos, los datos biométricos tienen mayor veracidad; no obstante, debe considerarse que las características de los individuos cambian con la edad, por lo que los datos biométricos no son infalibles y pueden ocasionar problemas de identificación

que quedan por fuera -aquellos que no son “nativos digitales”-, no solo del mecanismo particular, sino de todo lo que ello conlleva en adelante.

Ello así, al no existir aparente opción, pues debiera obrar específicamente determinado el mecanismo de contralor, máxime asistiendo a que dicha información atraviesa de manera transversal toda la órbita de la Administración considerando los distintos estamentos, se filtra, se considera y se utiliza.

Lo que se reclama es un modo de hacer la gestión de los datos, con el objeto de controlar qué se hace con ellos. Claro está, y conforme se ha referenciado, existirán matices o segmentos de relevancia en ese contralor, ello en tanto algunos datos estarán más próximos a la intimidad del individuo o de los colectivos sociales, y sobre ellos es donde deberá recaer la mayor intensidad de los procesos de gestión sin obviar que, actualmente, a través de la implementación de la inteligencia artificial, con la recopilación y gestión -enlace- de datos, pueden crearse perfiles personales, cuyo uso extralimitado podría generar incluso mayores daños que los escindidos.

A modo ejemplificativo, y para dar continuidad a la casuística referenciada en los párrafos precedentes, pues para ingresar a BOTI o para tramitar pasaporte o DNI en Renaper, todo ciudadano debe informar correo electrónico y número de teléfono celular. Ahora bien, ¿Conoce el ciudadano el alcance que dicho dato tendrá? ¿Con que fines será utilizado? En idéntico razonamiento, ¿Puede el ciudadano optar por no colocar dicho dato privativo? La operatoria es automática, absorbe y no tiene escapatoria. Pues, siendo aún desconocidas las consecuencias de tamaña transformación, puede incluso que el ciudadano no tenga siquiera interés en los cuestionamientos, por lo que el deber de reglamentar e informar -educar al ciudadano- cobra aun mayor relevancia.

Tal situación, no solo forma parte de la agenda pendiente de la administración pública local, sino asimismo en el plano internacional y de otros países latinoamericanos, en los que la legislación vigente deviene insuficiente -cuanto menos- para atender a la actual revolución de datos y transformación digital, normativa que asimismo se encuentra en constante dinamismo por las vicisitudes propias de la materia.

En efecto, la “Buena Administración” impulsada por el CLAD hacia adentro de los Estados, se presenta como una obligación del Estado Democrático de Derecho, que impetra

de dotar de herramientas suficientes para una buena gobernanza, con miras a proteger los derechos humanos fundamentales y la dignidad humana. En ese contexto, no puede desoírse la marcada e imperiosa necesidad de incorporar la debida tutela de los datos personales en la gestión de la Administración Pública.

Frente a lo expuesto, y a la evidente necesidad de adaptar la normativa imperante en nuestro país -aunque mejor posicionada internacionalmente que otros países latinoamericanos-; debe adicionarse la realidad fáctica actual, puesta en consideración en el choque entre la norma literal y la actividad efectiva de la Administración Pública, pues los limites surgirán -hasta tanto- de la adecuada ponderación legislativa del operador y de un procedimiento implícito delimitado por prácticas.

Ya lo refiere Arroyo Jimenez[6] "el Derecho administrativo es un Derecho de conflictos, especialmente entre principios constitucionales, cuya resolución presenta esa naturaleza y se articula técnicamente a través de la ponderación(…)El Derecho administrativo es, en definitiva, un Derecho de equilibrios entre principios constitucionales que frecuentemente generan conflictos llamados a ser resueltos en primer lugar por el legislador democrático mediante la elaboración de ponderaciones legislativas".

No con ello se interpreta que la Administración deba autorregularse hasta que la normativa se adapte a las nuevas realidades; sino que en ella y sus operadores radica la facultad de ponderación de las normas a la luz del bloque normativo, estándares internacionales, principios legitimantes y su adaptabilidad a la nueva realidad que nos circunda.

Frente a ello, deviene dable referenciar la teoría de la tópica jurídica como método aplicativo en el derecho público -analizada por DIEZ SASTRE en torno a la teoría de Viehweg-, entendida como técnicas de razonamiento jurídico para arribar a la solución de problemas, o técnicas de búsqueda de premisas para la argumentación jurídica (producto de la dialéctica y el consenso), entendiendo que el derecho parte de problemas concretos y no de sistemas.

[6]ARROYO JIMENEZ, LUIS. "Ponderación, proporcionalidad y Derecho administrativo". Revista para el análisis del derecho. Madrid, 2009. Pg. 24.

En la era contemporánea y sobre todo globalizada, esta metodología ha cobrado preponderancia para resolver problemáticas en el ámbito del derecho administrativo-, y que pretende aplicar la ponderación en la toma de decisiones, ello a través de tres ejes fundamentales: la función tópica de los conceptos jurídicos -entiende a los conceptos ´jurídicos´ como herramientas útiles para el pensamiento jurídico más allá de su caracterización, es decir "ofrecen un punto de vista con el que buscar una solución", como "ideas que ayudan a la discusión"; ejemplificado mediante el principio de proporcionalidad con sus elementos: idoneidad, necesidad y proporcionalidad en sentido estricto-, las técnicas tópicas de resolución de problemas ligados a estos conceptos -esencialmente tópicas- y la utilización de aforismos en el derecho público (recurso de argumentación en lugares comunes), -como máximas jurídicas comúnmente aceptadas, vinculadas al sentido común, materiales y no formales.

Ello interpela a inclinarse por un razonamiento de conceptos universalmente aceptables y estructurados bajo premisas que se emplean a favor y en contra de lo opinable, respetando toda forma vinculada a la lógica contemporánea de lugares comunes. En efecto, la tópica está al servicio del conocimiento del obrar humano para orientar su conducta y, pues, la norma positiva debe descansar sobre una racionalidad nutrida de lugares comunes. En ese sentido, vgr., comprender el tópico de "interés público" que habilita el tratamiento de datos personales por parte del derecho público, reclama comparar, interpretar y sistematizar un estándar mínimo, incluso comparando ordenamientos, para arribar a un razonamiento argumentativo lógico y devenido de lugares comunes.

La situación y panorama actual refleja y pone de manifiesto la transversalidad de los derechos humanos fundamentales en la vida de todos los Administrados y de la especial relación Estado-ciudadano, como así también la necesidad de adaptabilidad continua de todos los estamentos a un mundo cada vez más globalizado y con mayores avances tecnológicos; con su correlato en torno a su incorporación y aplicación en los procesos de la Administración, imponiendo nuevos desafíos en las relaciones y vínculos jurídicos y, sobre todo, en la protección y tutela de los derechos.

Ello debe asimismo amalgamarse con el novedoso acervo en torno al dato y la información al alcance, su debido uso y tratamiento y los organismos de contralor

específicos e imparciales, para la generación de políticas públicas concretas al servicio de la comunidad y una legítima toma de decisiones.

Cuando la Administración incorpora y desarrolla nuevas tecnologías -máxime cuando de recopilación y procesamiento de datos se trata- adquiere asimismo una responsabilidad especial y aumentada en torno a la tutela de los derechos de los administrados, debiendo suministrar y propender a un control más estricto y especiales garantías, incluso cuando los propósitos sean harto convincentes, pues no deja de ser interferencia en la vida privada de las personas; lo que no se amalgama con una sociedad democrática de derecho.

En ese sentido, emerge una mayor necesidad de ponderar proporcionalmente la legislación que resguarde los derechos, verificar la existencia de una organización determinada al efecto y un procedimiento afín, ello en miras de arribar a un equilibrio justo de salvaguardas suficientes.

Ciertamente, conforme se ha ido detallando e incluso se desarrollará seguidamente, Argentina no solo cuenta con una Ley Nacional de Protección de Datos Personales N° 25.326 y Decreto Reglamentario Nº 1558/2001; y su concurrente Ley Nacional N°27.275 de acceso a la información pública sino que, incluso, ha sido reconocida internacionalmente por el avanzando nivel de protección y tutela que la legislación refiere.

Ahora bien, el obstáculo que se advierte, además de la insuficiencia normativa y falta de adecuación en la gestión de datos por parte de la Administración –organización y procedimiento-, es la ausencia de normativa específica en la materia en la provincia de Entre Ríos, es decir que se vincule con la idiosincrasia de lo local, lo que interpela a hacer valer los estándares internacionales por vía constitucional y, claro está, refleja una -aún más marcada- insuficiencia y carencia de adecuación en la gestión de los datos personales para el sistema administrativo entrerriano.

A modo ejemplificativo, y con el objeto de entrelazar lo antedicho con la imperiosa necesidad de un procedimiento y organización afín al tratamiento y uso de los datos personales, puede referenciarse la vigencia local del Decr. Nº 1169/05 GOB que aprueba el “Reglamento General de Acceso a la Información Pública para el Poder Ejecutivo Provincial”, cuyo fin es regular el mecanismo común de acceso a la información pública,

estableciendo un marco general para su desenvolvimiento, esto es: sujetos alcanzados, mecanismo de solicitud, plazos de respuesta, responsabilidades y excepciones; todo ello enmarcado en motivaciones -obrantes en el propio acto administrativo- vinculadas a la Convención Interamericana contra la Corrupción, el principio de publicidad de los actos de gobierno y derecho de acceso a la información pública, vigentes en nuestra Constitución Nacional y el Art. 5 de nuestra Constitución Provincial.

Ciertamente, el Reglamento no prevé ni anticipa el 'objeto' del derecho de acceso a la información que podrá requerirse, es decir no parametriza si la misma contempla todo tipo de soporte –vgr. fotos, grabaciones, soporte magnético o digital-, mas sí lo determina como toda información que concierna a la comunidad, y no con cada uno de los ciudadanos individualmente considerados (aquí se deja por fuera el dato privado). Tampoco prevé la sistematización de la información para cumplir con los recaudos de la norma, esto es cómo ha de procesarse el dato para ser entregado (sea en forma de estadística o indicador). Aquí, mandatoriamente atraviesa la protección del dato personal y sensible por cuanto el dato duro aun no procesado exige un cabal entendimiento de la escisión que debe realizarse previo a su otorgamiento. Se verifica como ambas normas se erigen como limitantes una de la otra.

Véase que la hipótesis se presenta casi análoga, existiendo normativa nacional y parámetros internacionales que operan de basamento para regular -en este caso- el acceso a la información pública. Nuevamente, procedimiento y organización se presentan como la lógica y razonable solución para encausar un mecanismo común y adecuado.

Sin perjuicio de lo expuesto, resulta imperioso referenciar que (atendiendo a los casi 20 años de vigencia del Decreto, previo a la reforma constitucional provincial), recientemente, fue enviado para tratamiento legislativo provincial, un proyecto de ley de acceso a la información pública que, entre otras, prevé la creación de un órgano específico de centralización de información, dotado de potestades para controlar -en forma escindida- la información que se brindará a los peticionantes, ello con basamento en el Art. 13 de la Constitución Provincial del año 2008[7] y en los estándares propuestos por el modelo de la

[7] Art. 13 CPER: Se reconoce el derecho al acceso informal y gratuito a la información pública, completa, veraz, adecuada y oportuna, que estuviera en poder de cualquiera de los poderes u órganos, entes o empresas del Estado, municipios, comunas y universidades. Sólo mediante una ley puede restringirse, en resguardo de otros derechos que al tiempo de la solicitud prevalezcan sobre éste, la que deberá establecer el plazo de reserva de dicha información. La información será recopilada en el medio de almacenamiento de datos de acceso más universal que permita la tecnología disponible. Toda persona afectada en su honra o reputación por informaciones maliciosas, inexactas o agraviantes, emitidas en su perjuicio a través de un medio de comunicación social de cualquier especie, tiene el derecho a

OEA (presunción de publicidad, máxima divulgación de la información en forma regular y proactiva, garantía de reglas justas, acceso gratuito, y la obligatoriedad de justificación para el caso de negativa)[8]

Si bien la norma aún no ha sido tratada, deviene dable hacer mención de dos aspectos fundamentales vinculados a la temática del presente trabajo.

El primero de ellos en cuanto a una de las 'excepciones' para la carga de brindar información, a saber: "Información que contenga datos personales y no puedan brindarse aplicando procedimiento de disociación, salvo que cumpla con las condiciones de licitud previstas en la ley 25.326 de protección de datos personales y sus modificatorias". Se evidencia que la remisión a la normativa nacional de protección de datos personales, si bien comienza a considerar una tutela específicamente determinada, no hace más que relevar a la Administración de la efectiva tutela que prevén los estándares internacionales (consentimiento previo y derecho a la autodeterminación informativa), norma que aún no se ha actualizado al *SoftLaw* internacional.

Seguidamente, se verifica que se crea un organismo 'Oficina de Acceso a la Información Publica', que funcionara en el ámbito del Ministerio de Gobierno y Trabajo, es decir un área con dependencia directa del Poder Ejecutivo y cuya autoridad máxima será designada por el Poder Ejecutivo, careciendo *prima facie* de la independencia necesaria para dotar de transparencia plena y la centralización organizada y sistemática del acceso íntegro y oportuno que se pretende, todo lo cual excede el marco del presente trabajo.

En idénticos términos, se resalta la existencia del Decr. Nº 58/06 HCD, modificado por Decr. Nº 029/17 CD, que hace lo propio para el Poder Legislativo. Esta última reforma incorporo la consideración ante el Área Legal de la Cámara de Diputados de la determinación acerca del carácter 'sensible' de la información requerida, sin ningún tipo de parámetro, nuevamente conceptos difusos y poco claros. No existe reglamentación sobre la temática por la Cámara de Senadores ni por el Poder Judicial[9].

obtener su rectificación o respuesta por el mismo medio. La mera crítica no está sujeta al derecho a réplica. La ley reglamentará lo previsto en la presente disposición.

[8] https://www.oas.org/es/sla/ddi/acceso_informacion.asp

[9] Información extraída del texto "El derecho a la información Pública en Entre Ríos". Dr. Matías A. Plugoboy en "Constitución de Entre Ríos. Logros y deudas a diez años de la Reforma Constitucional". Pág. 401 a 425. Ed. Delta Editora, año 2018.

En esa misma línea, puede referenciarse asimismo la Ley Provincial Nº 10.898 de implementación y utilización del Expediente Electrónico, documento electrónico, domicilio y notificación electrónica en el ámbito de la Administración Pública provincial y en el marco de los procedimientos administrativos, cuyo Decreto Reglamentario Nº 1737/22 GOB prevé un mecanismo para su implementación gradual, determinando procesos de capacitación, conceptos claves y la reafirmación de la tutela y resguardo de los documentos a los que se accede -con mas, claro está, el inescindible contenido tutelado- (idéntica situación acontecida en el ámbito del Poder Judicial con la implementación del Expediente Electrónico y la reglamentación pertinente, con profusas y constantes capacitaciones en la materia)

Conforme lo antedicho, y tal como se especificara a lo largo del presente trabajo, no cabe duda de la necesidad de reglamentación afín al debido tratamiento y uso de los datos personales; esto es una organización transversal puertas adentro de la Administración que indique el cómo proceder, que sistematice la manera de hacer las cosas.

En dicho entendimiento, la normativa referenciada en los párrafos precedentes no hace más que reflejar que estamos ante un cambio trascendental en lo que respecta a digitalización y accesibilidad; siendo los datos el mayor acervo tanto del Estado como así también de la ciudadanía, y su tratamiento de mayor preponderancia.

Se reclama tutela y protección adecuada, enmarcada en regulación específica, pero que no sea una mera adhesión normativa a un marco regulatorio que no considera la perspectiva de la organización y de los funcionarios y agentes públicos locales, siendo que son quienes -en definitiva- terminan justificando la limitada regulación e, incluso, la ausencia de especificidad; y hasta la injerencia estatal sobre la información apelando al "interés público", la "urgencia", la "seguridad pública", entre otras alegaciones de ese extremo.

Para ello, deviene imperioso interpelar los conceptos que se utilizan para validar estas intervenciones en un escenario posmoderno -máxime cuando son los mismos ciudadanos los que lo reclaman-. No puede la Administración, o mejor dicho, el Derecho Administrativo, pretender trazar los límites a la inmunidades del poder y, a la vez, exceptuarse de su ejercicio dentro del bloque de la gestión política del Estado -quien en definitiva toma las decisiones-, pues lo público nunca "masifica" o parametriza (vgr. bajo el formato excusatorio: "interés

público") para "habilitar" injerencias que siempre serían arbitrarias si avanzan sobre ese aspecto de la vida de las personas o delos colectivos de personas, sino que siempre exige detenerse en las singularidades y garantizar su integridad, máxime considerando que la vinculación del sujeto con la sociedad se da en el plano de la reproducción digital como práctica social intensa que alimenta las redes en el plano local e internacional.

El sujeto (Administrado) es un usuario dotado de derechos, que opera hoy como componente fundamental del sistema en red, inescindible de su apreciación.

Ello así, se interpela a la equidad desde la Administración, que lo que se reciba en consideraciones de "justicia" no solo refiera a la igualdad para acceder al control, sino de lo que es adecuado hacer respecto de la naturaleza de la información personal y de la inexistencia de criterios ambiguos para justificar intervenciones (aún controladas) que permitan accesibilidades por terceros que comprometen calidad o condiciones de vida de las personas a las que esa información refiere o de las que trata.

Sin duda, estamos ante un derecho en formación (autodeterminación informativa) que reclama una adecuación asertiva no solo de la reglamentación -hoy desactualizada-, sino también de firmes procedimientos y efectiva organización que garanticen la efectiva tutela de aquello que queremos salvaguardar, comprendiendo que los conceptos son dinámicos y convergen en la era de la tecnología y la información de manera acelerada e incesante.

Existe una aceptación generalizada del fenómeno de invasión en la vida privada, como consecuencia de ser parte de la sociedad digital; con más que todos los procesos de las organizaciones estatales y no estatales han virado hacia las TCIs[10] -de uso masivo y generalizado-, por lo que la estrategia debe centrarse en tutelar el derecho en emergencia.

Ahora bien, de lo antedicho también deviene innegable que la ciencia jurídica debe darse el debate de definir si el uso masivo de las TICs, aportando claro está datos personales, debilita el derecho a la autodeterminación informativa o, en su caso, hasta qué punto. Ello por cuanto el mundo ha cambiado, las personas se relacionan a través de los sistemas, el gobierno es electrónico y la toma de decisiones es cada vez más automatizada (con

[10]Tecnologías de la Información y la Comunicación.

basamento en perfiles derivados de la aplicación de inteligencia artificial que acelera los procedimientos).

Incluso, ello impacta en todos los poderes estatales, por cuanto la sanción normativa no puede desvincularse de las realidad imperante en torno a las nuevas necesidades del ciudadano digital; con mas que las decisiones judiciales –cuando analizan reclamos por ilegitimidad de los actos administrativos- deben considerar asimismo las nuevas formas de ser de la Administración indagando, a pedido de parte u oficiosamente, si ha existido intromisión en la vida privada o se ha violentado la autodeterminación informativa.

La temática atraviesa todos los estamentos del poder, e impacta en la toma de decisiones plasmadas en actos, leyes o sentencias. La inexistencia de normativa de adhesión local no es óbice para la aplicación del derecho.

En efecto, en no mucho tiempo las nuevas generaciones desconocerán otra manera de hacer las cosas que no sea "virtual". Pues sus efectos aún se desconocen, como así también los peligros a los que se pueden quedar expuestos al proporcionar *inocentemente* los datos personales, por lo que -se insiste- es la ciencia jurídica la que deberá evaluar el concepto de "bien común" en la era posmoderna para legislar al respecto.

II. MARCO TEÓRICO CONCEPTUAL.EL ESTADO DE LA CUESTION

Actualmente, el manipuleo de los datos por parte de los registros públicos y diversas áreas de la Administración que toman contacto directo con los mismos encuentra un marco o bloque normativo concreto y especifico, determinado en la Ley Nacional de Protección de Datos Personales N° 25.326 -que data del año 2000- y su Decreto Reglamentario Nº 1558/2001, legislación que contiene los principios generales relativos a la protección de datos, los derechos de los titulares, las obligaciones de responsables y usuarios, el órgano de control -que ha sufrido modificaciones- y las sanciones y procedimiento del recurso judicial de *habeas data* normativa que, asimismo, se conjuga con la Ley Nacional N° 27.275 de acceso a la información pública; que impetra marcar el límite entre la transparencia y la protección de los datos -y su normativa local ya referenciada en el capítulo precedente-.

En efecto, la acción de *Habeas Data* encuentra hoy amparo en el Art. 63 de la Constitución Provincial, y habilita el acceso a los datos referidos a la persona interesada, su fuente, finalidad y destino, que consten en todo registro público o privado, con la salvedad

que la acción no procederá cuando la obtención de datos reclamados estuviese reglamentada[11]. Ciertamente, la herramienta se presenta como una garantía individual, cuando el 'dato' ya ha ingresado a la órbita de la Administración, y reclama una acción para su acceso, rectificación o destino, nuevamente cuando el daño quizá ya ha sido infringido.

Sin desmerecer la loable herramienta citada, de lo que aquí se trata es de la necesidad de articular un sistema interno de reglamentación que prevea, anticipadamente, un correcto uso y manipuleo de esa información, recabando el consentimiento previo y respetando el derecho a la autodeterminación informativa, concepto este último que se detallara en adelante.

Por su parte, la provincia de Entre Ríos no ha adherido a la Ley de Protección de Datos, por lo que actualmente la normativa aplicable se vincula directamente con los estándares internacionales que se referenciaran *infra*; el Art. 43 de la Constitución Nacional y el Art. 13 de la Constitución Provincial que refiere a las herramientas legales para la protección y tutela de la información respectiva a las personas que vulnere su honra y honor.

En efecto, a dicha normativa debe añadirse el bloque legal establecido e incorporado a nuestro derecho interno, conforme determina nuestra Constitución Nacional, en los Tratados Internacionales de Derechos Humanos con jerarquía constitucional, en tanto los Arts. 1 y 2 de la Convención Americana sobre DD.HH. expresamente refieren a la manda de los Estados Parte de hacer respetar los derechos y libertades allí reconocidos y de adoptar disposiciones de derecho interno para garantizar su efectivo ejercicio como así también, en su Art. 11, prevé la protección legal a la honra y la dignidad, sin permisión abusiva de injerencia en la vida privada[12].

Esas normas, a la luz del Art. 75 inc. 22 de la CN, gozan de jerarquía constitucional, a las que deben adicionarse los comportamientos deseables de los Estados o expectativas de conductas determinadas por el *SoftLaw* internacional, como fuente material del Derecho

[11] Art. 63 CPER: Toda persona tiene derecho a interponer acción expedita, rápida y gratuita de hábeas data para tomar conocimiento de los datos referidos a ella, a sus familiares directos fallecidos, o a sus propios bienes, así como la fuente, finalidad y destino de los mismos, que consten en todo registro, archivo o banco de datos público o privado de carácter público, o que estuviesen almacenados en cualquier medio técnico apto para proveer informes. En caso de falsedad o uso discriminatorio de tales datos podrá exigir, sin cargo alguno, la inmediata rectificación o actualización de la información falsa o la supresión o confidencialidad de la sensible. El ejercicio de este derecho no puede afectar las fuentes de información periodística ni el secreto profesional. La acción no procederá cuando la obtención de los datos reclamados estuviese reglamentada.

[12] Pacto de San José de Costa Rica: https://www.oas.org/dil/esp/tratados_b-32_convencion_americana_sobre_derechos_humanos.htm.

Administrativo, que en el último tiempo ha cobrado preponderante fuerza aplicativa al punto tal de ser un fenómeno de creación del derecho en la sociedad contemporánea; en tanto devienen como reglas y principios con incidencia en los ordenamientos internos por su intrínseco valor para el intérprete del derecho.

Deviene imperioso referenciar que la Decisión de la COMISIÓN DE LAS COMUNIDADES EUROPEAS de Bruselas de fecha 30/06/2003, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo sobre la adecuación de la protección de los datos personales en Argentina -hoy derogada- estableció, en su Art. 1°, que: "A efectos del apartado 2 del artículo 25 de la Directiva 95/46/CE, se considera que Argentina garantiza un nivel adecuado de protección por lo que respecta a los datos personales transferidos desde la Comunidad….", ello con basamento en la normativa vigente a nivel nacional, considerando la Constitución Nacional y la Ley de Protección de Datos.[13]

La importancia de este reconocimiento radica en la facilidad al momento de realizar transferencias internacionales de datos personales y habilita nuevas posibilidades de innovación e inversión en nuestro país.

Ahora bien, en 2018 entró en vigencia en Europa una nueva normativa que introdujo muchos cambios en materia de protección de datos personales; lo que posiciono a la Argentina en una incómoda situación puesto que, al no cumplir con estos nuevos estándares, la Unión Europea podría modificar su criterio y considerar que Argentina ya no es más un país con protección adecuada. De allí, la necesidad de actualizar la legislación.

Sumado a ello, en el año 2015 el Comité Jurídico Interamericano de la OEA emitió un informe que redefine los principios rectores en el marco de la privacidad y protección de datos personales, haciendo énfasis en que los mismos regirán en el ámbito público y privado. Dicho informe parte de la premisa que el procesamiento de datos debe serlo con fines legítimos y por medios justos y legales; especificando los fines de la recolección de datos y el consentimiento, haciendo hincapié en el principio de autodeterminación informativa, confidencialidad, protección y seguridad.[14]

[13]Decisión de la Comisión de las Comunidades Europeas de Bruselas. Año 2003 http://www.hfernandezdelpech.com.ar/PDF-%20comisionComuniEuropeas-ProtecDatosPers.pdf

[14]CJI Res. 212/15. Protección de Datos Personales. http://www.oas.org/es/sla/cji/docs/CJI-RES_212_LXXXVI-O-15.pdf

Por su parte, en el año 2016, se gestó en el seno del Honorable Congreso de la Nación un anteproyecto de ley que modifica la normativa actual, y que impetra por dotar de una regulación más moderna y que se amalgame con los cambios tecnológicos, ello en consonancia con el nuevo Reglamento (UE) 2016/679 del PARLAMENTO EUROPEO [15]y del CONSEJO del 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a su libre circulación, y por el que se deroga la Directiva 95/46/CE mencionada anteriormente. Dicho proyecto de ley no prospero por haber perdido estado parlamentario, pero sirvió de antecedente para ulteriores proyectos.

En efecto, dicho Reglamento establece como principio rector que la protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental, y que ello debe servir a la humanidad, no concibiéndose como un derecho absoluto sino en relación con su función en la sociedad, debiendo mantener el equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad.

Ciertamente, refiere que la rápida evolución tecnológica y la globalización han planteado nuevos retos para la protección de los datos personales, en tanto que la magnitud de su recogida e intercambio han aumentado de manera significativa y la tecnología permite que, tanto las empresas privadas como las autoridades, utilicen esos datos en una escala sin precedentes a la hora de realizar sus actividades, todo lo cual reclama un elevado nivel de protección.

Sumado a ello, se ha tenido como parámetro rector a los Estándares de Protección de Datos Personales para los Estados Iberoamericanos establecidos en el marco del XV Encuentro Iberoamericano de Protección de Datos de la Red Iberoamericana de Protección de Datos y que tratan, entre otros asuntos, de impulsar y contribuir al fortalecimiento y adecuación de los procesos regulatorios en la región, mediante la elaboración de directrices que sirvan de parámetro para futuras regulaciones o para la revisión de las existentes [16]; al que se ha sumado el Informe del Comité Jurídico Interamericano, actualizado, sobre Privacidad y Protección de Datos Personales [17], cuya finalidad es proteger a las personas de

[15]Reglamento 2016/679 del Parlamento Europeo y del Consejo del 27 de abril de 2016 https://www.ugr.es/sites/default/files/2017-08/CELEX_32016R0679_ES_TXT.pdf

[16]Estándares de Protección de Datos Personales para los Estados Iberoamericanos de la Red Iberoamericana de Protección de Datos: https://www.redipd.org/sites/default/files/inline-files/Estandares_Esp_Con_logo_RIPD.pdf

[17]Informe N° 638/21 del CJI sobre Privacidad y Protección de Datos Personales: http://www.oas.org/es/sla/cji/docs/CJI-doc_638-21.pdf

la recopilación, el uso, la retención y la divulgación ilícita o innecesaria de datos personales, proporcionar una guía para orientar la reflexión al interior de cada Estado miembro de la OEA sobre el estado de su normativa en la materia como así también, en su caso, los esfuerzos de fortalecimiento de la misma.

En el mes de junio de 2023 el Poder Ejecutivo Nacional informo acerca del tratamiento en comisión de un nuevo Proyecto de Ley para modificar la normativa vigente -en relación a la protección de datos personales-, ello con basamento en idénticos estándares internacionales de protección de datos personales, de los cuales se referencia el Reglamento General de Protección de Datos (RGPD); el Convenio 108 del Consejo de Europa para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal y su versión modernizada; las Recomendaciones sobre ética de la inteligencia artificial de la organización de las Naciones Unidas para la educación, la ciencia y la cultura (UNESCO); los avances a nivel regional como los "Estándares de Protección de Datos Personales para los Estados Iberoamericanos" de la Red Iberoamericana de Protección de Datos (RIPD); las legislaciones de la República Federativa del Brasil y la República del Ecuador; los proyectos de ley de la República de Chile, la República del Paraguay y la República de Costa Rica.

Sobre el particular, resulta imperioso referenciar la sanción de Ley 27.699 del año 2022 que aprobara el Protocolo modificatorio del convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (Convenio 108+), siendo Argentina uno de los primeros países latinoamericanos en ratificar el protocolo antedicho el cual impetra por proteger a cada persona, cualquiera sea su nacionalidad o residencia, con respecto al tratamiento de sus datos personales, contribuyendo así al respeto de sus derechos humanos y libertades fundamentales y, en particular, el derecho a la privacidad. Entre sus considerandos, el Convenio obliga a cada Parte firmante al tratamiento de datos sujeto a su jurisdicción en los sectores público y privado, garantizando así el derecho de toda persona a la protección de sus datos personales.[18]

[18]Sesión N° 128 del Comité de Ministros (Elsinor, Dinamarca 17-18 de mayo de 2018) - Comité Ad Hoc sobre Protección de Datos (CAHDATA) - Protocolo modificatorio del Convenio para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal (ETS No. 108) - Informe explicativo

Durante el decurso de esta investigación se encuentra en tratamiento el Proyecto de Ley referenciado.

Sumado a lo expuesto, resulta dable referenciar que el 22 de febrero de 2024 la Comisión de trabajo sobre "Gobernanza de Datos y Protección de la privacidad", la cual pertenece al Consejo Federal para la Transparencia[19] -constituido por un representante de cada una de las provincias y un representante de la Ciudad de Buenos Aires, y está presidido por la Directora de la Agencia de Acceso a la Información Pública (en adelante AAPI)-, elaboró el "Plan de Protección de Datos Personales". El objeto principal de este documento es el de formular planes específicos de protección de datos personales que contribuyan y faciliten la implementación de una cultura de la privacidad en cada uno de los organismos públicos.

Con ese fin, el "Plan de Protección de Datos Personales"[20] profundiza en distintas cuestiones tales como: marco legal vigente: se remarca la importancia de la Ley 25.326 de Protección de Datos Personales y su reglamentación, subrayando la necesidad de actualizarla con el fin de armonizar estándares regionales e internacionales, definición y tratamiento de Datos Personales: incorpora la definición amplia de datos personales, incluyendo datos sensibles, y se enfatiza en su tratamiento responsable dentro del sector público, respetando las normativas existentes y garantizando la seguridad y privacidad, datos Personales como Derecho Humano: reafirma la protección de datos personales como un derecho humano fundamental, promoviendo la autodeterminación informativa y el control personal sobre la información compartida, desarrollo de un Plan: insta a cada organismo público a desarrollar un plan integral que incluya políticas, procedimientos, y prácticas éticas para la gestión de datos personales, asegurando su protección efectiva y el cumplimiento normativo, política de privacidad: señala la importancia de establecer políticas de privacidad claras y accesibles, delineando responsabilidades específicas en el tratamiento de datos, estableciendo líneas claras sobre la finalidad del tratamiento, caducidad, cesión, transferencia internacional de datos, confidencialidad, medidas de seguridad, derechos de los titulares, entre otros, alojamiento en la nube: aborda la creciente relevancia del alojamiento en la nube, exhortando a una selección cuidadosa de proveedores que cumplan con altos estándares de seguridad y

[19] Creado por Art. 29 ley 27.275

[20] https://www.argentina.gob.ar/sites/default/files/documento_datos_2023.pdf

privacidad, especialmente en contextos de transferencias internacionales de datos, avances y desafíos futuros: apunta la necesidad de fortalecer la formación de planes de protección de datos, mejorar la capacitación interna y promover la concienciación pública sobre la importancia de la privacidad de los datos.

A ello debe añadirse la resolución 47/ 2018 de la AAIP 21, que plantea una lista de medidas recomendadas de seguridad que se pueden implementar, relacionadas a la seguridad y la completitud e integridad de los datos recolectados, la minimización de errores, la limitación del acceso no necesario para asegurar la confidencialidad; el control de los accesos definiendo responsables y responsabilidades, verificación y aplicación de controles, gestión de accesos, asignación de permisos, verificación de identidad, monitoreo, establecer procedimientos para el respaldo y la recuperación, gestión de vulnerabilidades, detección de incidentes de seguridad, y gestión de los mismos, entre otras medidas.

Sobre el particular, deviene imperioso poner de manifiesto que la provincia de Entre Ríos no forma parte de dicha comisión de trabajo.

Ello así, conforme el marco regulatorio vigente en nuestro país, aún no adaptado a las nuevas realidades circundantes y al derecho administrativo global en la materia, el manejo estatal de los datos personales se presenta como de amplia discrecionalidad. Ello presenta, a entender de esta parte, como insuficiente al bloque legalmente establecido para un debido tratamiento de los datos personales en la órbita de la Administración Pública; máxime en el ámbito local que se investiga, ello por cuanto el propio texto de la ley actual prevé situaciones de excepción para el uso y manipuleo de la información que hoy en día, con las afluentes tecnológicas, surgen como insuficientes.

Resulta suficiente revisar el Art. 5 de la normativa nacional vigente, que exime del consentimiento del particular para el tratamiento de los datos personales cuando los mismos se obtengan de fuentes de acceso público irrestricto, se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal; fórmula por demás imprecisa y que no pone límites razonables a las operaciones. O, en su caso, el Art. 11, inc. 3) del mismo cuerpo legal, siendo que asimismo exime del consentimiento para la cesión de

[21] Resolución 47/ 2018. Medidas de Seguridad - Tratamiento y conservación de los datos personales en medios Informatizados. Disponible en: https://www.argentina.gob.ar/ normativa/nacional/resoluci%C3%B3n-47-2018-312662

datos cuando se realice entre dependencias de los órganos del Estado en forma directa, en la medida del cumplimiento de sus respectivas competencias.

Surge manifiesto que, el tratamiento actual de los datos por parte del Estado-de amplio espectro-, en relación a eximir del consentimiento casi en un listado infinito de excepciones a la regla, no se condice con el principio rector en el ámbito internacional y de referencia para el debido manipuleo que reclaman los avances tecnológicos y que, primordialmente, posicionan al consentimiento como esencial -antes o en el momento que se recopilen los datos-, aseverando incluso que debería especificarse la identidad y datos de contacto del responsable, las finalidades específicas para las cuales se trataran los datos, el fundamento jurídico que legitima el tratamiento y los destinatarios o categorías de destinatarios.

Se evidencia una palmaria dicotomía entre ambos universos normativos; siendo que en el plano internacional el consentimiento es la regla, y las excepciones solo las legalmente previstas, incluso interpretadas con criterio restrictivo, mas en el plano nacional -y local por derivación-, la falta de previsiones específicas al respecto brinda un manejo discrecional de la cuestión, de amplio espectro.

Ciertamente, dicho tratamiento casi irrestricto de la información ha encontrado su contrapeso local, al menos jurisprudencial. Así, en el año 2018 la Cámara en lo Contencioso y Administrativo Federal declaró en el fallo "Torres Abad" (2018) [22]que, no requerir consentimiento para recolectar datos que serán utilizados en funciones propias del Estado equivale a una liberación en blanco que resulta excesiva, por lo que debe haber una restricción.

Este límite -según se desprende del referido fallo- debe ser que únicamente puedan recabarse y ceder datos sin consentimiento cuando se trate de datos recopilados con fines de defensa nacional, seguridad pública o represión de delitos. Para todo lo demás, habrá que obtener la autorización del titular del dato o encuadrar la situación en otra excepción de la ley.

[22] Fallo CAMARA CONTENCIOSO ADMINISTRATIVO FEDERAL- SALA V Expte. Nº 49.482/2016/CA1 "TORRES ABAD, CARMEN c/ EN-JGM s/ HABEAS DATA" Buenos Aires, julio de 2018.
https://cpdp.defensoria.org.ar/wp-content/uploads/sites/4/2017/10/Fallo-Camara-Contencioso.pdf

En el caso en estudio, la actora pretendía -mediante la acción de *habeas data*- que se preserve la confidencialidad de la información brindada a la ANSES, evitando la utilización de sus datos personales obrantes en la base del organismo previsional para otras finalidades distintas a aquellas que motivaron su obtención.

Dicho reclamo de la accionante surge a partir de la cesión de datos estipulada en la Resolución Nº 166-E/2016 de la Jefatura de Gabinete de Ministros, por la cual se aprobó el Convenio Marco de Cooperación entre la Administración Nacional de Seguridad Social y la Secretaría de Comunicación Pública.

En los considerandos de dicho reglamento se indicó que los motivos de la recolección de información se sustentan principalmente en que la mencionada Secretaría debe mantener informada a la población a través de diversas modalidades, que incluyen desde las redes sociales y otros medios de comunicación electrónicos, hasta el llamado telefónico o la conversación persona a persona, de forma de lograr con los ciudadanos un contacto individual e instantáneo. Asimismo, se señaló que resulta esencial para el Estado Nacional la identificación, evaluación y análisis de problemáticas o temáticas de interés en cada localidad del país, así como la comprensión y detección de variables sociales y culturales que permitan incorporar la diversidad federal en la comunicación pública.

En tal contexto, la cláusula segunda del referido convenio establece que "para el logro de los objetivos expresados en la cláusula primera, previo requerimiento, la ANSES remitirá periódicamente la siguiente información que obre en sus bases de datos: a) Nombre y Apellido; b) DNI; c) CUIT/CUIL; d) Domicilio; e) Teléfonos; f) Correo Electrónico; g) Fecha de Nacimiento; h) Estado Civil; i) Estudios.".

Se evidencia la extralimitación a las potestades del Estado sobre la recopilación y tratamiento de los datos -justificada en el ejercicio de su función-, sin consentimiento previo, reflejándose como sumamente interesante el análisis que se efectúa sobre la autodeterminación de la cesión informativa por parte del ciudadano y el contralor que debe existir cuando el Estado se extralimita en las facultades de tratamiento por una interpretación amplia de la normativa hoy aplicable.

Ya lo refiere BASTERRA, en torno a que "todo Banco o Registro público o privado, que desee tratar datos de personas físicas o jurídicas, como regla general deberá requerirles

previamente su consentimiento para el tratamiento, salvo que los datos se encuentren en alguno de los supuestos legales que eximen del mismo y, sólo con una interpretación restrictiva de la ley se logrará la efectiva protección del derecho a la autodeterminación informativa".[23]

Ahora bien, del análisis del anteproyecto mencionado *ut supra (2023)*, asimismo se evidencia que la "satisfacción de un interés legítimo" será considerada condición válida para la licitud del tratamiento de datos por parte de las autoridades. De esta manera, el Estado gozaría nuevamente de amplia discrecionalidad para tratar los datos de los ciudadanos que posea en sus bases, en tanto la noción de "interés legítimo" adolece de la suficiente vaguedad como para justificar diversos tipos de utilización de información personal. Los límites aún continúan difusos y poco claros, máxime considerando que diariamente el Estado manipula bases masivas de datos.

Sí se destaca el establecimiento de la "responsabilidad proactiva" para los responsables del tratamiento de datos, ello en torno a adoptar políticas de privacidad o adherirse a mecanismos de autorregulación vinculantes y el tratamiento de los datos por defecto, ello así que sólo sean utilizados los datos relevantes a los fines concretos.

Sin dudase torna ilusorio, cuanto menos, siendo que ello recaería en el propio organismo o autoridad que utilizará la información, generando en consecuencia una llamada "expectativa de confianza" en el operador de turno, de su capacitación en la temática y buen proceder.

Los mecanismos reglamentarios, de políticas públicas concretas y de gestión en torno a la toma de decisiones con base en el manipuleo de datos; no solo deben considerar la normativa imperante, sino también cómo ello ha sido reglamentado a nivel internacional y cuáles son sus principios rectores, por cuanto la constitucionalización del derecho administrativo se evidencia en las nuevas fuentes que producen derecho, en las reiteradas voces de la judicatura en torno a la preeminencia de los derechos humanos fundamentales y de la interpretación de las normas para una aplicación convencional del derecho en la toma

[23]BASTERRA, MARCELA. "El consentimiento del afectado en el proceso de tratamiento de datos personales". Jurisprudencia Argentina. Número Especial, 28 de abril de 2004, pág. 6

de decisiones, tanto fuera de la Administración como puertas adentro para su organización y los procesos de protección.

A decir de REYNA[24], el nuevo derecho administrativo contemporáneo se presenta como contra hegemónico, trasciende fronteras y abandona la jerarquía piramidal para inmiscuirse en un sinnúmero de sistemas normativos guiados por la Carta Magna. El entrecruzamiento transversal de otras normas que exceden lo doméstico obliga, a la Administración, a una práctica inescindible de los derechos humanos y del hombre como centro de toda decisión razonablemente considerada.

En esa línea de pensamiento, ciertamente podría considerarse la situación actual como un espacio administrativo global disperso, en el sentido que la efectiva determinación del tratamiento de los datos personales en el plano domestico impacta en lo global, ello por cuanto el manipuleo de esa información trasciende el territorio e ingresa en otro espacio gubernamental. Su contralor debe guiarse por los mismos principios rectores generales del derecho internacional, que fundan y fundarán la regulación actual y venidera del valor del dato digital, como así también el acceso irrestricto, por parte de los Estados, a los fines legitimados.

Concomitantemente, esa reglamentación determinada por la normativa internacional, pero de aplicación local, no es más que el cumplimiento del Estado de sus obligaciones internacionales convencionales. En ambos supuestos, el destinatario es el mismo: el individuo y su dignidad como eje central.

Lo dicho en los párrafos precedentes obliga a analizar el estrecho vínculo entre la Administración local y el efectivo espacio administrativo global, con un fin determinado y especifico, principios idénticos y mecanismos afines; siendo que uno se nutre del otro casi con prescindencia de los Estados "parte" y en una evidente proliferación de conductas, asimismo internacionales, que no componen el *HardLaw* internacional sino que son consecuencia directa de objetivos comunes, pautas de conducta y mecanismos de interpretación.

[24]REYNA, JUSTO J. "Globalización, pluralidad sistémica y derecho administrativo: apuntes para un derecho administrativo multidimensional". Revista de Derecho Administrativo y Constitucional. Ed. Forum. Belo Horizonte, 2011

Efectivamente Abramovich refiere a lo abordado, específicamente detallando la posibilidad del Sistema Internacional de Derechos Humanos (SIDH) de influir en las políticas públicas, en tanto sus principios se incorporen en las políticas de gobierno, en la elaboración de leyes y en las sentencias de tribunales locales, ello siendo que las decisiones adoptadas internacionalmente sobre un caso puntual, informes temáticos u opiniones consultivas imponen obligaciones de hacer a los Estados, enmarcadas en políticas públicas concretas o decisiones jurisdiccionales, cuyo imperativo radica en no desconocer la pertenencia internacional y evitar incumplimientos, siendo ello demostrativo que la reglamentación de dichas temáticas, vinculadas a derechos humanos, no puede escindirse del plexo normativo internacional por cuanto, de una u otra manera, su prescindencia impactará en el caso concreto y pondrá en evidencia a la Administración.

A modo ejemplificativo, la Res. N° 01/202 de la Comisión Interamericana de Derechos Humanos, referida a la Pandemia y Derechos Humanos de las Américas, en el Pto. C) "PARTE RESOLUTIVA, Inc. 12 "Derechos Económicos, Sociales, Culturales y Ambientales" reza: "Garantizar el consentimiento previo e informado de todas las personas en su tratamiento de salud en el contexto de las pandemias, así como la privacidad y protección de sus datos personales, asegurando un trato digno y humanizado a las personas portadoras o en tratamiento por COVID-19. Está prohibido someter a las personas a pruebas médicas o científicas experimentales sin su libre consentimiento" y en su Inc. 35 "Estados de excepción, restricciones a las libertades fundamentales y Estado de Derecho": "Proteger el derecho a la privacidad y los datos personales de la población, especialmente de la información personal sensible de los pacientes y personas sometidas a exámenes durante la pandemia. Los Estados, prestadores de salud, empresas y otros actores económicos involucrados en los esfuerzos de contención y tratamiento de la pandemia, deberán obtener el consentimiento al recabar y compartir datos sensibles de tales personas. Solo deben almacenar los datos personales recabados durante la emergencia con el fin limitado de combatir la pandemia, sin compartirlos con fines comerciales o de otra naturaleza. Las personas afectadas y pacientes conservarán el derecho a cancelación de sus datos sensibles…".

En otras palabras, recomienda enfáticamente a los Estados Parte de la Convención garantizar la privacidad y la protección de los datos personas en el tratamiento a su salud,

ello como un criterio y principio general en torno a toda reglamentación que, a nivel local, se adopte para mitigar los efectos de la Pandemia[25].

Dicha normativa internacional, a modo de recomendación, ha determinado en los Estados Parte la manda de limitar y restringir o, en su caso, amoldar, las medidas sanitarias locales en torno y miras a garantir el derecho a la protección de datos personales. Puntualmente, una regla de la gobernanza global es directamente aplicable a lo local y a la Administración doméstica, reflejada en medidas específicas que afectan a los individuos en todas las esferas, en este caso protegiendo los datos sensibles vinculados a la persona en su integridad y dignidad como sujeto de derechos.

En ese mismo orden de ideas, la incorporación de la provincia de Entre Ríos en la Agenda 2030 de la Organización de las Naciones Unidas para el Desarrollo Sostenible que impetra, a través de 17 objetivos de desarrollo sostenible y metas universales, orientar a los países suscribientes para lograr un desarrollo que cumpla con el mandato de la Agenda, en su Objetivo 16. 10 determina: "Promover sociedades pacíficas e inclusivas para el desarrollo sostenible, facilitar el acceso a la justicia para todos y crear instituciones eficaces, responsables e inclusivas a todos los niveles, Garantizar el acceso público a la información y proteger las libertades fundamentales, de acuerdo con las leyes nacionales y los acuerdos internacional" posicionando, de este modo, un mandato global *(SoftLaw*) en una política pública concreta aplicable a lo local, orbita provincial, y propiciando la protección del acceso a la información en pos de ser considerado, el Estado Parte, como cumplidor del mandato de la Agenda, sin efectivo rigor sancionatorio pero bregando por el sostenimiento de la reputación internacional.

Nuevamente, el vínculo se plantea como mandatorio.

Incluso, el Consenso de Andorra del CLAD (2020)[26](Centro Latinoamericano de Administración para el Desarrollo), organismo público internacional respaldado por la Asamblea General de las Naciones Unidas, que tiene por objetivo construir una entidad regional centrada en la modernización de las administraciones públicas, cuyo lema es "*Innovación para el Desarrollo Sostenible -Objetivo 2030. Iberoamérica frente al reto del Coronavirus*" especificó, en el Pto. 18 del compromiso asumido por sus Estados miembros,

[25]Res. N° 01/202 de la Comisión Interamericana de Derechos Humanos. 10.04.2020. https://cdh.defensoria.org.ar/normativas
[26]https://clad.org/wp-content/uploads/2020/10/Consenso-Andorra-PT-10-2020.pdf

la manda de: "…*garantizar siempre la privacidad y la protección de datos a través de marcos legales que se ajusten a los desafíos de la evolución tecnológica…*". Nuevamente, se posiciona a la protección de datos como una manda de y hacia los Estados.

Ciertamente, conforme lo establece Broun Isaac en su publicación titulada "Desafíos constitucionales en torno a la tutela del derecho de acceso a la información y libertad de expresión en la era digital", dentro de los desafíos de la meta y objetivos referenciados (ODS) se identifica la responsabilidad del Estado frente a los peligros contra la intimidad y la tutela de la privacidad.[27]

En consonancia con lo expuesto, y ratificando el valor del dato (información con valor agregado) y su trascendencia en la aplicación de políticas públicas concretas y toma de decisiones, a principios del 2021, la Corte Suprema de Justicia de la Nación se expidió en autos: "Gobierno de la Ciudad de Buenos Aires c/ Estado Nacional (Poder Ejecutivo Nacional) s/ acción declarativa de inconstitucionalidad" mediante el cual el Gobierno de la Ciudad Autónoma de Buenos Aires solicitó la declaración de inconstitucionalidad del art. 2º del decreto de necesidad y urgencia (DNU) 241/2021 del Poder Ejecutivo Nacional, que modificó lo dispuesto en el art. 10 del decreto 235/2021 y estableció -en su último párrafo- la suspensión del dictado de clases presenciales y de las actividades educativas no escolares presenciales en todos los niveles y en todas sus modalidades, desde el 19 hasta el 30 de abril de 2021, inclusive, en el ámbito del aglomerado urbano denominado "Área Metropolitana de Buenos Aires (AMBA)" por entender que la norma impugnada violaba de manera flagrante lo dispuesto por la Constitución Nacional, en cuanto garantiza el respeto de la autonomía de las provincias mientras estas aseguren la educación primaria (art. 5º), y garantiza y establece específicamente la autonomía de la Ciudad de Buenos Aires (art. 129), haciendo lugar al planteamiento.

En dicho resolutorio, si bien el basamento para hacer lugar a lo requerido se centró en lo normado en el Art. 129 de la CN y en un criterio sostenido por la Corte en torno a la paulatina concreción del mandato constituyente de conformar una Ciudad Autónoma de Buenos Aires con autonomía jurisdiccional plena; pues asimismo hizo uso de normativa internacional directamente aplicable al caso concreto en torno al derecho a la educación de

[27]BROUN ISAAC, JORGE TOMAS. "Desafíos constitucionales en torno a la tutela del derecho de acceso a la información y libertad de expresión en la era digital". ANUARIO DE DERECHO CONSTITUCIONAL LATINOAMERICANO. AÑO XXVI, BOGOTÁ, 2020, PP. 749-771, ISSN 2346-0849.

los niños constitucionalmente consagrado (Art. 75, inc. 22 CN); a los que se adiciona como fuerte cuestionamiento al endeble justificativo o fundamentación del DNU argüido, la escases de datos empíricos y tangibles que hicieran lugar a tamaña decisión.

En efecto, he aquí donde cobra implícito valor el dato concreto, específicamente determinado y que, en su caso, podría rebatir un decisorio. El dato se refleja como crucial para la toma de decisiones, máxime en un contexto de pandemia. Ahora bien, los mecanismos de recopilación, mediante sistemas y organización predeterminada que refleje un obrar homogéneo y ajustado a derecho, son cruciales para una correcta utilización de dicha herramienta.

Si bien, claro está, la Corte se limita a decidir acerca de la competencia sobre la incumbencia de CABA y el Estado Nacional sobre la temática, y no se inmiscuye en torno a la procedencia de las medidas sanitarias; pues especifica que ello no puede efectivamente hacerlo por cuanto el dato concreto que fundara el decisorio no surge del instrumento traído a debate, evidenciándose -en consecuencia- como una decisión deliberada y antojadiza que, además, avasalla competencias.

En esta instancia surge palmaria la importancia del dato, su debido análisis y tratamiento, en otras palabras, ¿hubiera sido otro el desenlace de haberse acompañado datos empíricos concretos y tangibles que justificaran la toma excepcional de decisiones? ¿ello hubiera motivado la aplicación del principio de razonabilidad y proporcionalidad? Ya se especificaba al inicio de la emergencia sanitaria la igualdad de prevalencia que debía darse a las medidas de prevención, como así también a los testeos y rastreos; por cuanto el dato es inescindible de la política pública -sanitaria en este caso- a aplicar en el caso concreto.

Sin lugar a duda, toda debida recopilación de datos debe estar dotada de un procedimiento concreto, específico, organizado e idéntico; para hacer un uso adecuado y legítimo de la información a la que se accede.

El dato es una herramienta preponderante de la gobernanza, que mide el humor social, las realidades particulares, los anhelos, gustos, intereses y necesidades; de allí la imperiosa necesidad de su debido tratamiento. No puede prescindirse del acceso al dato como un factor necesario para la aplicación y generación de políticas públicas y de reglamentación (con enfoque en los derechos humanos), como así también para la toma de

decisiones que impactan en la vida social, pero, como tal, asimismo debe reglamentarse debidamente su uso legítimo por parte de la Administración.

En consonancia con ello, deviene dable referenciar que el desarrollo jurisprudencial en los distintos sistemas internacionales de derechos humanos ha sido mucho más rico respecto del derecho a la vida privada que relativa al derecho a la protección de datos personales.

De hecho, hasta el momento, la CIDH no se ha pronunciado de manera explícita en ningún caso respecto del derecho a la protección de datos personales, a pesar de que un gran número de países lo contemplan en su derecho interno como derecho humano. Ello así, la protección de datos personales se produce a nivel regional, sentándose criterios y estándares internacionales y determinando obligaciones positivas de los Estados para proteger los datos personales.

De esta manera se ponen de manifiesto las asimetrías que se presentan por región en cuanto a su reconocimiento y alcance, con más la ausencia de criterios internacionales uniformes, todo lo cual interpela a generar estándares homogéneos a nivel global, con autoridades de control independientes, principios y deberes que legitimen su tratamiento y el control efectivo de la información; impulsando la confianza por intermedio de una protección adecuada.

Actualmente, y sin perjuicio de la normativa nacional vigente, el bloque normativo internacional relacionado a la protección de los datos personales y los proyectos de reforma y adaptación de la ley a los parámetros internacionales de tutela de la integridad y privacidad; surge como tamaño desafío -máxime en la era de las telecomunicaciones y de la circulación al instante del dato digital- interpelar a sus operadores a balancear la efectiva necesidad de acceso a la información para llevar a cabo procesos de transformación y mejoramiento administrativos para el desarrollo de políticas públicas y la efectiva protección de los datos en poder de la Administración Pública, con una implícita manda de reserva de la información por imperativo legal, ético y moral.

Estamos en presencia de la denominada Sociedad Digital, que presenta nuevas plataformas de flujo de información y que, paralelamente, reclama nuevos mecanismos de protección tanto para datos personales como para datos sensibles.

En este océano de información los datos son vistos como una infraestructura en sí mismos y, las grandes cantidades de datos "Big Data" se convierten en factores de producción esenciales tanto para empresas privadas como para organismos públicos y, sin perjuicio de quien lo detente, la realidad fáctica es que el valor del dato se ve reflejado en la proliferación de la tecnología del conocimiento, como capital de los Estados -de todo estamento- para el desarrollo de la economía y el nivel de competitividad.

Subestimar el dato, reduciéndolo solo a lo empírico, seria desconocer el efectivo impacto en el mejoramiento de la calidad de vida de la sociedad. El debate gira, entonces, en torno a la pertinencia del usoy gestión del dato desde la Administración Pública; y a no perder el foco en la protección de los derechos humanos.

En efecto, en el mes de febrero de 2020 la Corte de Distrito de La Haya dicto una sentencia sobre el Sistema de Indicación de Riesgos (SyRI) de inteligencia artificial, con basamento en el Art. 8 del CEDH (Convenio Europeo de Derechos Humanos) que propugna el respeto a la vida privada; fallo que cuestiona y pone en jaque la utilización de sistemas de gestión pública basada en algoritmos, poniendo límites a su legislación y a la utilización gubernamental de la inteligencia artificial en miras de proteger el derecho a la privacidad y la protección de datos personales.

Dicho sistema de riesgo, de creación y utilización en los Países Bajos, busca colaborar con la investigación y constatación de fraude al sistema de seguridad social, pero la Corte entendió que la utilización de dicho mecanismo contraría el derecho humano a la vida privada, toda vez que implica un injerencia directa del gobierno en la privacidad de las personas, sin respetar los principios básicos de proporcionalidad y necesidad, le impone el carácter de "espionaje masivo", añadiendo que el desarrollo de SyRI tiene un efecto discriminatorio y estigmatizador, con mas que carece de transparencia en torno al modelo algorítmico que resulta de una recogida masiva de datos.

Ello así, no puede desconocerse que la normativa debe estar a la altura de la realidad imperante y que los alcances de la información a la que accede la Administración, a través de la toma y recopilación (tratamiento) de datos, se presentan como ilimitados; razón por la cual, para garantir su re-direccionamiento en beneficio de aumentar la eficiencia del sector público, deben establecerse concretos y específicos lineamientos para su uso en debida forma, máxime cuando de automatizar decisiones se trata.

Sobre este punto, es muy ilustrativa la Sentencia del Tribunal Constitucional Alemán de 27 de febrero de 2008[28], sentencia que es el resultado de un recurso contra la Ley de los Servicios de Inteligencia del Estado de Renania del Norte- Westfalia. Con la reforma que se impugna se permitía que los servicios de inteligencia utilizaran en "*forma secreta spywares troyanos para espiar en los ordenadores de cualquier sospechoso*". El Tribunal "*declara inconstitucional la reforma y configura, por primera vez lo que se ha considerado ya como un nuevo derecho fundamental a la confidencialidad e integridad de los sistemas tecnológicos de información. El Tribunal de Karlsruhe da así un paso más en el reconocimiento, primero, del derecho a la autodeterminación informativa y más tarde del derecho a la protección absoluta de la zona nuclear (corearea) del comportamiento privado (prívate conductoflif)".*

El Tribunal relaciona directamente el derecho de los individuos a la vida privada, a la libertad y expresión de la personalidad con los límites que debe tener el poder del Estado, al afirmar que "*El individuo depende de que el Estado respete las expectativas justificables de confidencialidad e integridad de tales sistemas de cara a la irrestricta expresión de su personalidad*", y ello significa que "*este derecho a la integridad y confidencialidad de los sistemas tecnológicos de información (...), que nos permite "tener una idea sobre partes relevantes del comportamiento vital de una persona u obtener una imagen representativa de su personalidad (...) sólo puede ser restringido en casos muy limitados*."

O, en su caso, otro fallo del mismo Tribunal del año 2020[29], referido al derecho a la privacidad de las telecomunicaciones y libertad de prensa, vinculada al Servicio de inteligencia federal, espionaje a periodistas y telecomunicaciones extranjeras. La queja constitucional se dirigió principalmente contra las nuevas disposiciones legales que permitían al Servicio de Inteligencia Federal recopilar, almacenar y analizar datos en el contexto de la vigilancia o espionaje de las telecomunicaciones en el extranjero así como también las disposiciones que autorizan al Servicio de Inteligencia Federal a transferir la información obtenida de alguna entidad pública nacional (especialmente de la policía y de fiscalías) o bien extranjera y de entidades privadas.

[28]Caso BvR 256/08, BvR 236/08 y BvR 568/708. Tribunal Constitucional Federal de Alemania.

[29]Caso 1BvR2835/17. Tribunal Constitucional Federal de Alemania.
En https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2020/05/rs20200519_1bvr283517.html

Ello así, el Tribunal entendió que "*Las medidas de espionaje interfieren en la protección de los derechos fundamentales que deben ser garantizados de acuerdo con el art. 1.3 LF. Eximir a los servicios de inteligencia de proteger los derechos fundamentales de extranjeros en otros países no se corresponde con la Ley Básica. El efecto vinculante integral de los derechos fundamentales, de conformidad con el art. 1.3 LF, crea el marco en que se pueden tener debidamente en cuenta los riesgos que corre su protección frente a los nuevos desarrollos tecnológicos; en particular en el contexto de la creciente importancia de los servicios de inteligencia, que va aparejada de los avances tecnológicos que facilitan su expansión en terceros países*" (…) "*Las disposiciones impugnadas son formalmente inconstitucionales, ya que autorizan interferencias violatorias de la privacidad en las telecomunicaciones de acuerdo con el art. 10.1 LF, y no cumplen con el requisito dispuesto en el art. 19.1.2 LF de especificar expresamente los derechos fundamentales afectados es impedir que se los debilite por medio de interferencias*" (…) "*Es por ello que el legislador debe disponer medidas que restrinjan y especifiquen el volumen de datos que pueden circular por las rutas respectivas, y debe delimitar el área geográfica cubierta por el espionaje. Debe estar plasmado detalladamente en la ley que la comunicación interna o aquella en que estén involucrados ciudadanos alemanes o residentes en Alemania sea debidamente filtrada en condiciones científicas y tecnológicas óptimas. En los casos en que no fuera posible, la eliminación debe ser llevada a cabo de forma manual. Las excepciones deben limitarse al máximo*"(el subrayado me pertenece).

El Tribunal da un paso más, un peldaño estructural, mandando a modificar la normativa imperante en pos de los principios protectores del derecho humano fundamental a la privacidad.

No existe libre albedrío del Big Data fundado en interés público o fin social, por cuanto el límite está impuesto en el derecho a la privacidad y el consentimiento informado para su circulación, con conocimiento pleno e informado de los alcances que tendrá el uso de esa información, siendo mandatorio tener en claro diversos conceptos para saber qué y cómo reglamentar, sistematizarlos y unificarlos.

Frente a ello, y como contrapeso de la necesaria reglamentación del tratamiento debido de los datos, se presenta la obligada mecanización de procesos de transparencia en lo que respecta al acceso a la información pública y, para lograrlo, la utilización de datos

personales -no sensibles- que faciliten su alcance, sin con ello violentar los límites de la ley de protección de datos; lo que ahora halla su correlato en la Ley de Transparencia N° 27.275.

Bien lo afirma Griffero[30], en su trabajo investigativo vinculado al derecho de acceso a la información pública en Argentina y el derecho de protección de datos personales; quien refiere enfáticamente que, ante la existencia de un conflicto (entre acceso a la información pública y protección de datos personales), la resolución vendrá de la mano de una ponderación razonada entre el interés público en conocer la información y la incidencia que la divulgación de esa información puede tener sobre el derecho de los afectados.

Tal afirmación no quiere decir que la resolución será siempre en base a la casuística, sino que, como se aprecia en el sistema argentino, la Ley 27.275 estableció una remisión a los términos de la Ley 25.326 para orientar la solución. El sistema actual de la Ley de Acceso a la Información Pública impone en primer lugar que, cuando la información contenga datos personales, la misma debe entregarse disociada y, en caso de que esa disociación no sea posible, podrá negarse su entrega, salvo que se cumplan las condiciones de licitud previstas en la Ley 25.326.

Ciertamente, la temática en estudio ha cobrado especial relevancia desde la implementación, en el seno interno de los Estados, de las tecnologías de punta al servicio de la política y gestión gubernamental, ello con el objeto de construir un nuevo tipo de Estado, un "Estado de Bienestar Digital" (ONU 2019), generando una intrínseca vinculación con la recepción y tratamiento de los datos para el mejoramiento de la vida de las personas y, asimismo, la aplicación de políticas públicas concretas, cobrando primacía en el plano de la agenda mundial.

Ya en el año 1998 el CLAD trató la temática de promover el análisis en torno a la reforma del Estado y la modernización de la Administración Pública, publicando su propuesta de reforma gerencial para los Estados latinoamericanos bajo el título "Una nueva gestión pública para América Latina".

En dicho documento ya se especificaba la necesidad de modernizar la administración pública al servicio del ciudadano. A ello se han adicionado documentos e iniciativas del

[30]GRIFFERO, ANDRÉS. "El derecho de acceso a la información pública en argentina y el derecho de protección de datos personales. a propósito de la ley nº 27275". R.I.T.I. nº 4 Mayo-Agosto 2017.

Centro para impulsar estrategias de cambio, tales como la Carta Iberoamericana de la Función Pública (2003), Carta Iberoamericana del Buen Gobierno (2006), Carta Iberoamericana del Gobierno Electrónico (2007), que propugna el derecho de los ciudadanos a vincularse electrónicamente con la Administración y a simplificar los procedimientos y la interoperabilidad y la Carta Iberoamericana de los derechos y deberes del ciudadano en relación con la Administración Pública (2013), que posiciona al ciudadano como protagonista principal de los asuntos de interés general.

Seguidamente, el Centro publicó un documento vinculado a la Gestión Pública Iberoamericana del S. XXI, con una agenda modernizadora y su consecuente perfeccionamiento, poniendo énfasis en la democratización de la Administración Pública con un fin social, dando lugar al documento que expone la Transformación del Estado para el Desarrollo Iberoamericano, proponiendo la construcción de una institucionalidad estatal, brindando calidad a la gestión pública focalizada en la imparcialidad, la honestidad, la eficacia y la legitimación de obrar.

Este bloque de documentos, a los que Argentina ha adherido y acompañado, son el sustento *SoftLaw*-que reflejan el funcionamiento de la sociedad internacional- para la ulterior producción normativa y la adaptabilidad de las Administraciones, principios que deben y deberán regir toda legislación que vincule al funcionamiento de la administración digital venidera, máxime si de tratamiento de datos personales se trata.

Recientemente, se presentó un artículo académico en la Facultad de Derecho de la Universidad *Finis Terrae* de Santiago de Chile, que analizo la efectiva necesidad de un marco regulatorio de protección de datos personales y protección de la vida privada en dicho país.

Allí se puso en evidencia la ausencia de protección efectiva al valor del dato, como riqueza global, sobre todo en cuanto a la rapidez con que se actualizan las nuevas tecnologías, trayendo a colación el concepto de "autodeterminación informativa", esto es la facultad de las personas de decidir por sí mismas cuando, donde y dentro de qué limites revelar información de su vida privada, como así también el carácter dinámico del derecho de protección de los datos personales que reclama una reglamentación de calidad, que permita el tratamiento licito y transparente de los datos personales en consonancia con el

desarrollo tecnológico, invirtiendo la regla general de tratamiento de datos y la creación de un órgano específico de contralor y fiscalización.

Por su parte, un estudio publicado en la Revista de Derecho, Comunicaciones y Nuevas Tecnologías del sistema legal uruguayo de protección de datos personales revela que el nuevo diseño del mundo de la comunicación, que ha ido transformando a la información en un factor clave, interpela a tutelar en debida forma el derecho a la intimidad, siendo que el derecho a la protección de datos personales se presenta como un elemento esencial para el libre desarrollo de la personalidad de las sociedades democráticas, que propende a un flujo adecuado de información e, incluso, que la dinámica de las situaciones fácticas posicionan a la normativa actual como desactualizada.

En consonancia con ello, un estudio doctoral de la Universidad Complutense de Madrid, relativo al derecho fundamental a la protección de datos personales en México y la influencia del ordenamiento jurídico español, analiza el tratamiento de datos personales por parte de la dependencias y entidades públicas de México, poniendo de resalto los principios de licitud, calidad, acceso y corrección de información, seguridad, custodia y consentimiento para su transmisión; posicionando asimismo el consentimiento como factor fundamental para el manipuleo de la información, mas presentándose excepciones taxativamente especificadas; haciendo especial hincapié en la necesidad de homogeneizar la normativa internacional en la temática; ello atendiendo a que la instantaneidad de la era globalizada reclama una estandarización de las normas que tomen lo mejor de cada ordenamiento.

Efectivamente se da cuenta que, en los ordenamientos jurídicos latinoamericanos referenciados que tratan la protección y tratamiento de datos personales, se evidencia una excesiva permisividad hacia el Estado con relación al almacenamiento, tratamiento y cesión de datos personales, con más una endeble supervisión por parte de los órganos de contralor y la inexistencia de una unidad de coordinación, todo lo cual enfatiza aún más la necesidad de reflexión e investigación en la temática.

III. HIPOTESIS. OBJETIVO GENERAL Y ESPECIFICOS

Considerando la normativa vigente en nuestro país y aplicable al espacio local provincial en torno al acceso, tratamiento y divulgación de datos personales, se verifican difusos e insuficientes los limites frente al debido uso, manipuleo y gestión por parte de la

Administración Pública de la información a la que se accede, de carácter privativo y sobre la cual el Estado tiene el deber de garante, máxime considerando los procesos de digitalización y ordenamiento de base de datos que reclaman una asertiva regulación direccionada a la protección de los derechos fundamentales, constitucionalmente consagrados, vinculados con la identidad, integridad y vida privada.

A continuación, se plantea el Objetivo General y los Objetivos Específicos.

Objetivo general:

Indagar acerca de los limites existentes, en el ámbito de la Administración Pública local, en torno al acceso, tratamiento y divulgación de los datos personales protegidos por la Ley de Protección de Datos Personales, cuya guarda surge como manda del Estado, explorando los desafíos organizacionales, procedimentales y normativos para un correcto y asertivo método que considere los nuevos procesos de digitalización, almacenamiento de datos y acceso a la información.

Objetivo específico 1:

Identificar dinámicas organizacionales, procedimentales y jurídicas respecto del acceso, uso y manipuleo de los datos personales de la ciudadanía entrerriana por parte de la Administración Pública local. ¿Cuál es el modelo jurídico vigente en torno a la protección legal de los datos personales? ¿Detenta el Estado local un acceso irrestricto a dichos datos? ¿Cuál es el uso que la Administración Pública local efectúa de la información a la que accede? ¿Es un uso correcto según los estándares vigentes? ¿Existen organismos administrativos de contralor/fiscalización/sanción? ¿Existen procedimientos para proteger el acceso a los datos por fuera del conflicto particular? ¿Existe autorregulación Estatal?

Objetivo específico 2:

Identificar los principios orientadores internacionales en materia de acceso irrestricto a datos personales. ¿Cuál es el escenario internacional en torno a la protección de datos personales frente a la Administración Pública local y global? ¿Alcanza nuestro país los estándares internacionales para la protección de datos? ¿Es considerada Argentina un país seguro en torno al tratamiento transfronterizo de datos personales, conforme los estándares internacionales? ¿Sobreviene la informática una amenaza potencial como herramienta del Estado frente a la vida privada de los ciudadanos?

Objetivo específico 3:

Determinar los posibles efectos de una libre e irrestricta circulación de datos suministrados por parte de la ciudadanía a la Administración, como así también los desafíos venideros en la era de la "Administración Digital". ¿Conoce el Administrado el destino de los datos suministrados al Estado? ¿Qué consecuencias específicas acarrea la circulación de esa información privativa en poder de la Administración? ¿Implica el tráfico constante de información, sin la debida tutela, una violación al derecho a la intimidad y vida privada? ¿Qué implicancias detenta para el Estado la posesión del dato? ¿Es evitable, por parte del ciudadano, proveer el dato al Estado? ¿La protección del dato y los procesos de fiscalización implican un impedimento para la innovación?

A entender de esta parte, el tema seleccionado para abordar la investigación deviene de palmaria relevancia en lo que respecta a la Administración local actual y venidera; ello atento la innegable proliferación de la tecnologización y digitalización del Estado, sus componentes, operadores y mecanismos de vinculación con la ciudadanía; todo lo cual reclama un acabado conocimiento de los mejores procesos de contralor para evitar un uso equivocado del nuevo acervo: el dato digital.

En consonancia con ello, el valor del dato se presenta como fundamental, surgiendo como mandato su utilización en debida forma, ergo por operadores capacitados, con conocimiento de los límites y con un especifico órgano de contralor y fiscalización que evite prácticas ilegítimas y por fuera del fin social que debe darse a la información a la que se accede; con el horizonte en la dignidad humana y los principios rectores que enmarcan los estándares de la sociedad democrática de derecho.

Actualmente, los límites al tratamiento de los datos personales por parte del Estado local se evidencian difusos, poco claros, discrecionales y, sin duda, desconocidos por el ciudadano de a pie e incluso por operadores estatales; todo lo cual abre la puerta a un uso irrestricto y deliberado de la información.

Dicho estado de situación reclama una solución correcta y que se amalgame con los nuevos desafíos impuestos en la era digital, que no pueden dejar por fuera los estándares internacionales y el comportamiento de otros Estados en la temática, en un panorama en el que el Estado Constitucional se presenta con competencias concurrentes tanto en los

distintos niveles de gobierno (en el marco de un Estado Federal), como así también licuando fronteras e inhibiendo la exclusividad e inherencia, para que los deberes converjan en un común mandato de garantizar derechos, posicionando a la dignidad y la persona humana como centro.

Sin duda alguna estamos en la puerta de acceso a un nuevo tipo de Administración, que se ha ido gestando durante décadas, y que se relaciona con la inmediatez del vínculo Estado-ciudadano, ello a través de la electrónica y la tecnología de punta al servicio de la sociedad y; junto a ello, un nuevo derecho administrativo.

Pues tal acelerado avance, que ha encontrado un feroz impulso en el año 2020 como consecuencia de la Pandemia, impetra a una readecuación de la normativa imperante y de los procesos organizativos internos de todo Estado, que tenga en especial consideración al ser social y su dignidad, con perspectiva de derechos humanos y un viraje conductual por parte de los organismos de control y, asimismo, de los funcionarios y agentes del Estado receptores de datos; que refleje un acabado conocimiento de lo delicado de la cuestión y la importancia de un tratamiento acorde.

IV. METODOLOGIA

El presente trabajo, cuyo objeto es explorar los limites existentes en torno al debido uso y tratamiento que la Administración Pública local debe endilgar a los datos personales de la ciudadanía; se basará en una estrategia metodológica cualitativa y sincrónica, no experimental, con el énfasis centrado en la realidad imperante y los nuevos desafíos de la Administración Digital, cuyo método de producción de datos será a través del análisis de documentos como productos sociales, con el objeto de obtener resultados exploratorios.

Se intentará indagar, mediante una investigación básica y documental, acerca de las dinámicas organizacionales, procedimentales y jurídicas -esto último a través de la judicatura local, nacional e internacional- en torno al acceso, uso y manipuleo de los datos de carácter privativo de los ciudadanos por parte de la Administración Pública local; ello en consonancia con el marco normativo vigente, el sistema de contralor/fiscalización y el alcance de los principios y estándares internacionales. Para ello se analizará el sistema jurídico actual local, nacional e internacional y el comportamiento de otros Estados, estudiando asimismo las voces de la doctrina y la judicatura.

Las unidades de análisis serán, por un lado, los documentos a investigar y, por el otro, las prácticas discursivas, éstas últimas habidas a través de declaraciones, discursos políticos, fallos jurisprudenciales (nacionales e internacionales), *SoftLaw* internacional y estudios científicos en la materia o vinculados a la temática.

El método de análisis de las prácticas discursivas se verá reflejado en las opiniones mayoritarias y minoritarias obrantes en los documentos en análisis (bibliográficos y hemerográficos), esto es: debates en torno al proyecto de ley vigente, doctrina nacional e internacional, libros, trabajos de investigación y artículos jurídicos.

CAPÍTULO I: EL VALOR DEL DATO Y LA EFICIENTE GESTION DE LA INFORMACION EN LA ERA DIGITAL

1.-Sistema Organizacional actual de la Administración Pública local para la protección de datos personales.

Adoptándose el concepto de derecho administrativo esgrimido por MARIENHOFF, a saber: "…conjunto de normas y de principios de derecho público interno, que tiene por objeto la organización y el funcionamiento de la administración pública, como así la regulación de las relaciones inter orgánicas, interadministrativas y las de las entidades administrativas con los administrados"; puede advertirse que el derecho administrativo resulta un complejo sistema, compuesto por normas, principios y procedimientos direccionados a brindar un esquema conductual hacia adentro y hacia afuera que permita la regulación de la actividad pública y de las relaciones jurídicas de su ámbito de actuación.

En el caso en estudio, y a decir de BALBIN, debe interpelarse fuertemente la pirámide jurídica de prelación normativa, con el objeto de hallar los diferentes matices en torno a cuál es, no solo el conjunto de normas aplicables al caso concreto, sino también el procedimiento de creación y de interpretación.

A partir de la reforma constitucional del año 1994, con la incorporación al derecho interno de los tratados internacionales de derechos humanos -con jerarquía constitucional y en las condiciones de su vigencia-, se ha receptado un bloque legal complementario de los

derechos y garantías de nuestra Carta Magna. En ese sentido, dichos tratados se vinculan estrechamente con los principios de progresividad y no regresividad de los derechos, en tanto promueven el desarrollo de los derechos humanos como pilar fundamental.

El derecho administrativo, y particularmente en lo que respecta a las normas que reglamentan el uso, manipuleo y tratamiento de datos personales por parte del Estado, no es ajeno a la subsunción al sistema jurídico internacional de derechos humanos y a los estándares internacionales de conducta entendidos como el *SoftLaw* internacional, con peso cada vez más firme en la toma de decisiones de los Estados.

Ya se especificó, al inicio del presente trabajo que, necesariamente la reglamentación de la temática y la conducta de los operadores se vincula estrechamente con las recomendaciones de la Unión Europea en torno a las garantías de protección y tutela de la vida privada de las personas y su dignidad, lo que reclama sistemas de protección cada vez más fuertes y específicos.

No es menos cierto entonces que, sin perjuicio de la normativa vigente en la materia, debe estarse asimismo a los principios rectores conductuales en torno a la temática; y que atraviesan sin lugar a duda el comportamiento de los distintos organismos, funcionarios y agentes que lo componen; a lo que se adiciona el lineamiento moral que debe regir en toda toma de decisiones, máxime frente a la tutela de los derechos humanos.

Así como el derecho privado se autorregula en su accionar con el objeto de estar al nivel de los estándares internacionalmente aceptables; pues el comportamiento de la administración -sin perjuicio de la ley vigente que rija en la materia y su adhesión o no por la provincia- debe estar acompañado de la intrínseca incorporación de todo tipo de fuentes que se amalgamen con los estándares internacionales que tutelan los derechos.

Incluso, a dicho planteamiento -al que se adiciona la multiplicidad de situaciones que surgen de la temática en estudio y quizá hacen a la imposibilidad de reglamentar y legislar todos los supuestos-, se suma la necesaria existencia de un procedimiento de tutela basado en los propios estándares conductuales, con prescindencia de la vigencia normativa que lo determine, sino más bien en torno a la aplicación directa de los principios de progresividad y no regresión, como un procedimiento implícito, conductual y guiado por la sana crítica y la razonabilidad.

En otras palabras, el operador jurídico y el funcionario, incluso el agente estatal conoce -por cuanto es una derivación del razonamiento lógico y la ética- que los datos personales de las personas deben ser tutelados y tratados con suma cautela, por lo que un procedimiento acorde debería lograr amalgamar esos intereses para una correcta consecución de los fines. Ello así, la función del agente debe estar dada en custodiar con máxima seguridad y bajo sanciones muy severas en caso de filtración o uso indebido.

No debe obviarse que el ejercicio de la función pública se encuentra fundado en un servicio a la comunidad y no en un obrar antojadizo que permita el apartamiento discrecional a las reglas de conducta, sobre todo morales. La ética pública debe ser el pilar conductual fundamental y ejemplificativo que habilite un debido contralor de los procedimientos.

A decir de Villar Palasi, la mayor dificultad del derecho administrativo consiste en la ausencia de principios rectores válidos para la totalidad de su normativa jurídica. En efecto, el escenario de actuación de la sociedad contemporánea es radicalmente opuesto a aquella comunidad sobre la que se sentaron las bases de la construcción del derecho administrativo. El doctrinario incluso plantea la ruptura del concepto de "norma completa", considerándola como los elementos desgajados del ordenamiento jurídico, en tanto para aplicar derecho se deben buscar los elementos dispersos; en una visión tópica, desde el caso concreto.

Si bien el fin último emerge como común denominador, ergo la búsqueda de la paz social: Estado social de derecho y derechos fundamentales; ciertamente hoy en día el destinatario -administrado- se presenta en una realidad diferenciada, con mayores vinculaciones hacia otros estamentos, con necesidades inminentes de regulación de lo digital en torno a su actividad diaria y exigiendo a la administración una organización acorde a la nueva era, que le garantice una vida digna y una existencia adecuada a un mundo globalizado.

Ya lo refirió la CSJN en el fallo "HALABI"[31] en el que, si bien la Corte crea la acción de clase y le brinda efectos *erga omnes*, se pone de manifiesto el principio de solidaridad para garantir un derecho de dimensión colectiva en relación con la privacidad en el uso de internet y telefonía personal frente a posibles intromisiones de organismos del Estado.

[31] CSJN. 24.02.2009. Halabi, Ernesto c/ PEN ley 25.873 y decreto 1563/04 s/ amparo.

En el caso en estudio, el actor reclamo la inconstitucionalidad de la ley 25.873 y su decreto reglamentario en cuanto autorizaba la intervención de las comunicaciones telefónicas y de internet sin que una ley determine en qué casos y con qué justificativos. Sin duda alguna, rigen los principios básicos que interpelan a la Administración a un obrar acorde a la regla fundamental, lo que halla su correlato -a decir de BALBIN- en el postulado básico prohibitivo del modelo de derecho público, respecto de la actividad estatal en relación con los derechos de los particulares. El Estado no puede hacer, salvo que una ley lo autorice a ello y si esa ley es inconstitucional por flagrante violación de los derechos humanos; pues la pirámide jurídica obliga a dejarla sin efecto.

Deviene innegable que, hoy en día, emerge un nuevo tipo de conocimiento y escenario de poder, que es excluyente y que ha marcado una cultura auto comunicativa diferente, en la que debe ponerse sumo énfasis sobre el principio de legalidad de los actos administrativos.

Ahora bien, justamente son los principios base del ordenamiento jurídico administrativo, ante la ausencia de reglas precisas, los que deben tomarse como mandatos de optimización para resolver conflictos o situaciones problemáticas e incluso para interpretar conductas y brindar respuestas con sustento; a lo que debe adicionarse que los operadores jurídicos deben convertirse en agudos observadores de las transformaciones políticas y sociales devenidas del avance tecnológico al servicio de la administración y como eje fundamental y transversal en la vida de las personas.

A decir de ARROYO JIMENEZ, el derecho administrativo es un derecho de conflictos de construcción normativa, y de equilibrios entre principios constitucionales. En situaciones y escenarios de actuación en los que la Administración puede actuar con margen discrecional, dado por la normativa imperante en la materia, es asimismo donde entra a jugar el principio de proporcionalidad y los márgenes de apreciación.

En efecto, la Administración no es automática ejecutora de la ley -a mi entender, y en el caso concreto no operativa-, sino que su accionar reclama un proceso intelectivo y procedimental previamente diseñado al efecto, mayormente por cuanto su accionar impacta de lleno en la vida de los individuos. Dicho proceso, de interpretación de la ley en el Poder Ejecutivo, se encuentra teñido de la nota de discrecionalidad que le otorga libertad de obrar, por cuanto carece de reglas específicas y determinadas.

No puede desoírse que, bajo el nacimiento de las nuevas formas de comunicarse y de relacionarse ha surgido una relación social compleja entre el administrado (sea persona física o jurídica) y el Estado, en la que se vislumbra que el ser humano como ser social, si bien se auto gestiona a sí mismo a través de las múltiples herramientas y plataformas informáticas al alcance, reclama como correlato mayores necesidades de provisión de servicios y de reglas claras.

En otras palabras, sin el abastecimiento de servicios claves como internet, energía, telefonía y redes, que garantizan actualmente el acceso a turnos de hospitales, pagos de servicios, inscripciones en el sistema educativo, entre otros, se generaría una situación de caos y perturbación de la vida social que, actualmente, gira en torno a ese tipo de vínculos, en el que estar *online* es cuasi obligatorio.

Ya lo advertía Nuria Magaldi en su artículo "El concepto de procura existencial en Ernst Forsthoff y las transformaciones de la administración pública"[32], trayendo el concepto de Procura Existencial de Forsthoff, en tanto re-significación de las funciones estatales en la era de la posguerra, como un Estado que debe intervenir en la vida social para procurar la prestación de servicios esenciales para una vida digna y supervivencia, que ya no pueden auto-gestionarse los individuos por la mayor dependencia que genera formar parte de los grandes centros urbanos. Ya no es el individuo por sí solo suficiente para procurarse, y eso otorga a la Administración nuevos cometidos, valiéndose de los procedimientos y formas que el derecho le proporciona.

Esta novedosa asunción de las responsabilidades estatales podría asimilarse a esta nueva era, de revolución tecnológica, en la que el Estado tienen el deber de procurar y garantir un espacio de desenvolvimiento que garantice, en el marco de una relación social compleja Estado digital/individuo digitalizado, un efectivo ordenamiento y procedimiento que no avasalle las garantías y derechos fundamentales ya adquiridos.

Sumado a ello, y en parangón, pues ciertamente con la mayor responsabilidad estatal emerge un mayor poderío de la Administración -que detenta y hace uso del dato-; siendo inescindible de la existencia del sujeto, como parte integrante de la sociedad, brindar esa información para vincularse con el entorno, todo lo cual reclama un proceso organizativo

[32]MAGALDI, NURIA. "El concepto de procura existencial en Ernst Forsthoff y las transformaciones de la administración pública". Revista de Derecho Público: Teoría y Método. Madrid, 2020.

que se comporte con reglas claras de conducta. En tal cambio de paradigma deviene imperioso el análisis de las formas en las que el ser humano actual desarrolla su existencia y cómo ello impacta en las reglas de conducta vigentes.

Como se adelantara en la introducción del presente trabajo de investigación; el sistema jurídico en torno a la protección de datos vigente se presenta como insuficiente, en un análisis estrechamente vinculado a la realidad contemporánea de la que no puede escindirse la organización actual de la administración local y sus competencias, lo que reclama la asunción de nuevas obligaciones a los poderes públicos en torno a las tareas de protección y contralor en el uso y manipuleo de los datos; actividad que pareciera haber quedado relegada.

El derecho administrativo debe acomodarse a la realidad de su tiempo y, con ello, el énfasis debiera colocarse en la dotación de organismos de control con competencias claras, y en una rigurosa organización -hacia adentro- de fiscalización específica en la temática.

No puede negarse que la normativa actual, compuesta por la Ley Nacional de Protección de Datos Personales N° 25.326 -que data del año 2000- y su Decreto Reglamentario Nº 1558/2001, con más el bloque legal establecido e incorporado a nuestro derecho interno, conforme determina nuestra Constitución Nacional, en los Tratados Internacionales de Derechos Humanos con jerarquía constitucional -Arts. 1, 2 y 11 de la Convención Americana sobre DD.HH-, a lo que deben adicionarse los comportamientos deseables de los Estados o expectativas de conductas determinadas por el *SoftLaw* internacional; generan un compendio normativo que -en líneas generales- marca cierta suficiencia en torno a la protección de datos; mas ciertamente poco refiere en torno al especifico actuar de la Administración para a su tutela.

Incluso, es de destacarse que la ley referenciada, que data del año 2000, sufrió más de 80 modificaciones entre decretos y resoluciones, desdibujando su objetivo y habilitando su incumplimiento por parte del Estado. Sin duda alguna, se evidencia claro que la regulación legal para proteger los intereses de los ciudadanos en torno a la protección de sus datos avanza más lentamente que la tecnología que habilita la colecta desenfrenada de información.

Ciertamente, el objeto de la Ley 25.326 es la protección integral de los datos personales asentados en archivos o registros y el acceso a dicha información, en consonancia con el Art. 43 de nuestra Carta Magna, esbozando detalladamente un bloque de protección frente al usuario. Ahora bien, dicha normativa -hoy vigente- presenta algunas flaquezas que la hacen -quizá intencionalmente- permeable a un sinnúmero de excepciones (sobre todo para el Estado), y es allí donde radica la insuficiencia de tal plexo normativo para salvaguardar los intereses de los administrados.

En efecto, puede advertirse que el propio Art. 5 de la normativa mencionada exceptúa del consentimiento del particular para el tratamiento de datos personales 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 (…)". Sin lugar a duda, puede evidenciarse la generalidad y discrecionalidad con la que el articulado de la ley habilita al Estado al tratamiento de datos; referenciando el concepto de sus "funciones propias". Pues valga cuestionarse qué función que realiza la Administración, inherente a ella, no es "función propia".

En otras palabras, conforme la normativa vigente, el Estado puede acceder a los datos sin el consentimiento del particular, lo que se refuerza incluso con la excepción de recabar el consentimiento del particular para ceder los datos, cuando esa cesión se realice entre dependencias de los órganos del Estado en forma directa, en la medida del cumplimiento de sus respectivas competencias, sin que siquiera sea requisito la disociación de la información personal. Pues las competencias de los órganos estatales son dadas por el propio Estado.

No puede soslayarse que el consentimiento, conforme la estructura jurídica vigente, es una de las escasas intervenciones que tiene el particular titular de los datos respecto del complejo sistema organizaciones de lo público.

Ahora bien, conforme lo determina la normativa en estudio y la organización administrativa local actual –reiterándose que E.R. no ha adherido a la ley nacional-, ingresados los datos de los particulares a la órbita estatal (sea por cargar formularios, para acceder a servicios, para seguimiento de expedientes, para realizar peticiones o requerimientos, entre otros), se evidencia un sistema dual de "protección" indirectamente

gestado; ello en tanto la seguridad de dicha información recae tanto sobre el responsable o usuario -persona física-, como así también sobre órgano al que pertenece. Asimismo, a ello debe añadirse el control del manipuleo por parte de los organismos de fiscalización.

Ello así, el particular responsable -en este caso agente estatal- debiera adoptar las medidas técnicas y organizativas para asegurar la seguridad y confidencialidad de los datos personales mediante un mecanismo técnico de protección, como así también de la íntima convicción personal del sujeto en cuanto a la no divulgación; a lo que generalmente se acompaña la suscripción de un pacto de confidencialidad.

Como puede evidenciarse, el primer contacto del Estado con el dato es a través de sus operadores y en ellos radica el inicial filtro de seguridad. Huelga cuestionarse la suficiencia en torno a la capacitación de los agentes, el conocimiento de la normativa vigente, la especifica educación en la materia y la idoneidad puesta al servicio de la tarea endilgada; esto es la convicción moral y ética del sujeto -agente estatal- para no distorsionar el manipuleo de la materia prima ingresada.

Sobre ello no sería ilógico pensar en la aplicación de normas y reglas de conducta (códigos o estándares) derivadas del sector privado para el correcto funcionamiento y control, dentro del esquema actual colaborativo entre sector público y privado; como por ejemplo la incorporación de las normas ISO de derecho privado internacional a los procedimientos públicos, por estar dotadas de independencia y prestigio.

En ese sentido, y en el marco de un concepto de responsabilidad social aplicada a la gestión pública; entendida como la integración voluntaria de una organización (pública o privada) de la preocupaciones sociales, económicas y ambientales en sus operaciones y relaciones con demás interlocutores, con el objeto del desarrollo de objetivos sostenibles; podría pensarse en un mecanismo organizacional que tenga en consideración auditorias independientes bajo normas GRI (*Global Reporting Initiative)*o de "*Accountability",* como instrumentos (procesos) que cualquier organización puede seguir para contabilizar, administrar y comunicar su desenvolvimiento social y ético, de revisión administrativa y mejora continua.

No es un dato menor, al menos cuando pensamos en la creación de confianza como consecuencia directa de la aplicación de dichos procesos a la Administración, que favorece

en definitiva la concreción de políticas públicas consistentes y de calidad y a la toma de decisiones debidamente razonadas, que consideren los impactos en la sociedad, en este caso en la vida privada de las personas.

A decir de CANYELLES: "…para poder abordar los retos que el sector público tiene ante la ciudadanía, ante sus recursos humanos, y ante todos aquellos actores con quienes ha de cooperar, es necesario desarrollar la capacidad de crear confianza. No hay bastante con encontrar objetivos o intereses comunes, sino que este nuevo modelo requiere diálogo, transparencia, autenticidad (...) Requiere construir un nuevo perfil institucional en el que la responsabilidad sea un valor clave y donde esta responsabilidad se gestione activamente ante todos los grupos de interés que conforman la sociedad. En este contexto de tránsito desde el gobierno tradicional a un modelo basado en la gobernanza aparece la necesidad de gestionar la responsabilidad social de las administraciones públicas, como un reto central para mejorarla capacidad de crear valor social"[33].

Sobre el particular, impera cuestionarnos acerca de aquellos mecanismos que las Administraciones Públicas modernas deben desarrollar para mejorar la confianza de la ciudadanía hacia el Estado (tanto instituciones como funcionarios que las representan). En ese aspecto, la publicidad de la información y el mayor acceso a los datos públicos cobra un rol fundamental en brindar transparencia a los procesos; todo lo cual va de la mano del debido resguardo de dicho acervo. Los mecanismos de control (rendición de cuentas, escucha ciudadana, apertura y mayor justicia social) se han transformado en el eje fundamental de la participación en todas sus formas, incorporando al ser social en el andamiaje estatal; con la premisa de un gobierno abierto.

Esta circunstancia se replica en todos aquellos organismos estatales por los cuales atraviesa el dato; aquellos de mero pase y aquellos en donde se extrae y hace uso del acervo; máxime por la permeabilidad de la cesión de la información dentro de la propia organización. Ciertamente, el mecanismo de control continúa recayendo en la convicción interna del agente estatal, y el conocimiento que se detente del bloque de protección que obra detrás de tamaña información cobrando, la confianza en el aparato estatal, un rol fundamental.

[33]CANYELLES, JOSEP MARIA. Responsabilidad social de las administraciones públicas. Revista de Contabilidad y Dirección. Vol. 13, año 2011, Pág. 85

A ello podría añadirse ya la actuación de los jefes de Área/Departamento o funcionarios responsables jerárquicamente de cada organismo en los que se receptan datos, dotados de mayor deber de contralor, en el caso local por la Ley 9755, quienes efectivamente responden al órgano y son la cara visible del Estado, siendo su actuar consecuente al obrar de la Administración.

A modo ejemplificativo, deviene palmario traer a colación la reciente sucesión de hechos acontecidos dentro de la órbita de actuación del RENAPER (Registro Nacional de las Personas); organismo en el que se evidencio una fuga masiva de datos personales de más de 60.000 personas en fracción de segundos -ello para su ulterior venta, *prima facie*-; habiéndose constatado que ello fue consecuencia de un uso indebido de usuarios habilitados para el manipuleo de datos por parte del Ministerio de Salud de la Nación. Si bien, aparentemente, el obrar ilegitimo sería imputable a determinados agentes del ámbito de salud; no es menos cierto que la ocurrencia de un hecho de tal envergadura es consecuencia de la ausencia de organismos de control en torno a la temática y a la facilidad de acceso a la información, no solo intra-organismos, sino de los propios agentes estatales.

Ahora bien, sin ahondar en la temática da la responsabilidad administrativa, civil y penal por la divulgación y uso indebido de los datos, lo que merecería un estudio diferenciado y que no corresponde al objeto y extensión del presente, sí surge necesario al menos referenciar que la tarea de control y la responsabilidad devenida de su ausencia son conceptos, a entender de esta parte, inescindibles, y que deben ser considerados en el procedimiento que se implemente.

Surge como correlato especificar, conforme tiene dicho FIORINI[34], que el Estado aparece como la unidad organizada dentro de la cual se realizan los procesos que son necesarios en el Estado de Derecho, en otras palabras, los procesos y la organización hacen a la existencia misma de la Administración, de los que se nutre para su existencia. En ese sentido, el proceso administrativo, compuesto por procedimientos específicos dependiendo la materia, tiene como fin en sí mismo la realización estructurada de la voluntad estatal.

Sin duda alguna, la voluntad estatal de cada ordenamiento administrativo -sea nacional, provincial o municipal- viene dada por la Ley Fundamental como sustento univoco

[34] FIORINI, BARTOLOME. "El estado y los procesos estatales". Capitulo Segundo.

y común denominador, por cuanto no podría imaginarse un ordenamiento que contemple reglamentación que vaya en contra o en detrimento de la Carta Magna, y es por ello que el comportamiento, como funciones intrínsecas a cada estamento, no puede deslindarse de los principios rectores y de supremacía general del Art. 31 de nuestra Constitución Nacional.

En ese orden de ideas, la ya referenciada ausencia de regulación y ordenamiento efectivo en torno a la protección de datos a nivel local podría darse por dos factores: desconocimiento en la materia, puesto de manifiesto en la ausencia de educación/capacitación sobre el particular en todos los niveles; o falta de voluntad de cambio; como representativa de dar continuidad a la permeabilidad del uso indiscriminado de los datos por parte de la Administración, por su innegable valor. Ambos factores, incluso, pueden darse en forma concomitante dependiendo de la etapa procedimental y organizativa que se analice.

Probablemente el agente público que se desempeña en una mesa de entradas (incluso digital) y debe recibir y procesar la información/datos remitidos por el ciudadano de a pie para realizar determinada tramitación, desconozca *prima facie* los principios rectores de la ley nacional de datos y los estándares internacionales de tutela a la vida privada y la dignidad y, sin lugar a dudas, llegado el dato al área que pretende hacer uso de la información obtenida en forma indirecta para un fin determinado, sin el consentimiento del particular (ello habilitado por la ley vigente, como consentimiento táctico); vgr. cederlo a otro organismo estatal o ente autárquico, priorice el ejercicio de la función propia y las metas políticas de la gobernanza a tutelar el interés particular que, en principio, pareciera no estar vulnerado.

De ello se deriva que surge imperativa la necesidad de adoptar conocimiento y un procedimiento afín puertas adentro de la organización estatal; siendo que toda tecnología puesta al servicio de la Administración conlleva no solo los riesgos propios de la ausencia de discrecionalidad humana ante el oficio de la inteligencia artificial -permeable-, sino también del mal obrar de las personas, como individuos diferenciados que se extralimitan -a sabiendas o no- en el uso indiscriminado de la información a la acceden.

Por ello, uno de los severos planteamientos (y que incluso ha sido uno de los puntos de discusión de la normativa nacional); es si la organización del contralor debe ser jurisdiccional o debe estar centralizada en un organismo que no sea controlado por el poder

político. Entiendo que, en la primera hipótesis debiera al menos contar con autonomía e independencia.

Frente a ello, cabe señalar que el ordenamiento jurídico administrativo debe ser analizado, entonces, desde una fas subjetiva. Ello es, dando intervención al ciudadano en la relación jurídica administrativa, como sujeto de derecho, con el fin de brindar una debida tutela a los derechos individuales, con basamento en el principio de colaboración del individuo hacia el Estado (ruptura del concepto de "obediencia"), más que de la subsidiariedad. A decir de UTRILLA FERNANDEZ[35] "la aproximación en clave subjetiva al Derecho Administrativo no solo puede servir para proteger mejor al ciudadano frente a los excesos del poder, sino también para mejorar el ejercicio por parte de la Administración de las funciones que le son propias".

Sobre ello, también recae el deber del ciudadano de involucrarse -participar- en la organización estatal, no como mero espectador sino participando en la acción organizacional. Ya lo refiere PERLO, al teorizar sobre la necesidad de adoptar y construir una mente colectiva -la vida de grupo- para introducir el interaccionismo simbólico (lenguaje, palabras y conversaciones) a las teorías organizacionales, ello a partir de considerar las interacciones e influencias mutuas entre individuo y organización para construir la unidad organizacional, concluyendo que el comportamiento de las organizaciones jamás puede escindirse de los individuos que las componen, es más lo necesita para generar cultura de aprendizaje organizacional hacia adentro y hacia afuera.

Ciertamente, en la era contemporánea, el eje no debe centrarse -solo y estrictamente- en la actuación administrativa, su eficacia y control -plexo objetivo del sistema de derecho administrativo-, sino también abordando la relación jurídica entre Administración y sujeto administrado, máxime en temáticas como el particular, en las que se ahonda acerca del concepto de "interés legítimo" y "consentimiento" para adentrarse en los procesos internos de la Administración, en las que el individuo aparece en un rol activo en procura de la protección de sus derechos y no como mero espectador, con basamento en el principio de autodeterminación informativa, en torno a decidir el límite hasta el cual la información relativa a una persona puede ser objeto de procesamiento y tratamiento.

[35]UTRILLA FERNANDEZ- BERMEJO, DOLORES. "La relación jurídica en el sistema de derecho administrativo". Revista de derecho Público: Teoría y método. Madrid, 2020.

En definitiva, tanto la organización administrativa como el involucramiento del sujeto en dichos procesos y procedimientos repercuten en forma directa en la garantía de los derechos constitucionales, existiendo una relación intrínseca, inescindible y necesaria para su realización. En efecto, sin perjuicio de la tutela de los derechos individuales que recae como mandato sobre el Estado, son asimismo sus propios órganos y sus respectivas competencias -que caracteriza de válido al acto administrativo *per se*, por un actuar dentro de las atribuciones legales- los que ejercitan esa protección a través de su proceder cotidiano.

Emerge como propuesta, en consonancia con la necesaria innovación y transformación del Estado, abandonar el modelo de Estado burocrático tradicional -sobre la base del modelo weberiano de rígidas jerarquías y procedimientos estandarizados- a un esquema más flexible pero asimismo eficiente y capaz de satisfacer las demandas de los ciudadanos, a una reforma del Estado "hacia adentro", incorporando normas organizativas transversales que habiliten un efectivo contralor del uso y manipuleo de la información a la que se accede, habilitando la incorporación de procesos del sistema privado; articulando redes de conexión con otros organismos por fuera y dentro del estamento, con basamento en un procedimiento de registrar solo lo "necesario" (y determinar este concepto jurídica y administrativamente para justificar por qué es "personal/íntimo"); habilitando condiciones técnicas para una carga personal y no tercerizada por el funcionario; como así también el control del titular de esa información que se registró y el "olvido" del asiento cuando desaparecen las razones que justificaban la "tenencia" de esa información.

Sobre el particular, considero dable citar extractos del documento 'Lineamientos para la formulación de un Plan de Protección de Datos Personales' emanado del Consejo Federal para la Transparencia, ello en el marco de la Comisión de trabajo 'Gobernanza de Datos y Protección de la Privacidad' año 2023[36], a saber:

"El Estado en sus distintos niveles y el conjunto del sector público son hoy los actores que mayor cantidad de datos personales recopilan, almacenan o procesan. Cada vez más, las organizaciones públicas reconocen en los datos personales un activo estratégico. Nadie puede concebir una Estado inclusivo, eficaz, eficiente sin un tratamiento masivo de datos personales. El tratamiento de estos datos permite mejorar las prestaciones, acortar los tiempos, ser más eficientes y, en general, dota de mayor capacidad para lograr impactos sociales, económicos y ambientales para el bienestar de los ciudadanos…."

[36] https://www.argentina.gob.ar/sites/default/files/documento_datos_2023.pdf

"…Cuando hablamos de tratamiento de datos personales cada vez más lo estamos asociando a las nuevas tecnologías disponibles, como la inteligencia artificial y la inferencia de datos, que permiten no sólo mejorar la calidad de los servicios sino formular con más precisión el tipo y el alcance de las políticas públicas, proyectar incidencias y resultados. Al mismo tiempo que abre enormes oportunidades para el mejoramiento de las políticas públicas, implica también enormes responsabilidades y riesgos, pues el tratamiento de datos personales tiene implicancias en lo que hace a la seguridad, privacidad, y potenciales sesgos discriminantes. Es por eso que para el sector público es clave seguir los lineamientos legales y de responsabilidad pro activa. Al representar al conjunto de la comunidad, tiene mayor responsabilidad y pone en juego, a cada paso, su legitimidad, reputación y credibilidad. En este sentido, hay mucho por hacer…"

"…La gran mayoría puede identificar el flujo de los datos personales y trata datos sensibles. También se realizan habitualmente cesiones a otros organismos y una proporción considerable utiliza servicios en la nube. Esta situación evidencia la necesidad, en gran parte de las jurisdicciones, de avanzar en que cada organismo posea un plan de protección de datos personales, un manual de procedimiento interno, una política de Privacidad, y un DPO encargado del tema, así como en lo que respecta a protocolos de seguridad, capacitaciones internas y campañas de sensibilización. Sensibilización e información que debe ser extendida al conjunto de la población y en particular a grupos vulnerables. Por último, se destaca la relevancia en todos los organismos del sector público de enfocar la protección de los datos personales desde el diseño de las políticas públicas y durante todo el ciclo. Estos lineamientos para la formulación de un plan de protección de datos personales se proponen contribuir a estas tareas y ser de utilidad para la formulación del mismo, teniendo en claro que solo puede servir de guía, dado que cada provincia y cada organismo tiene su propia realidad y sus propias necesidades, lo que exige adecuar y adaptar estos lineamientos a los problemas concretos que cada sector enfrenta…"

Sin duda alguna, la problemática se ha enaltecido al punto de evidenciar la necesidad de elaborar un plan de acción, que maximice las responsabilidades éticas estatales en torno a la protección de datos personales en el sector público; en tanto se reitera: el procedimiento y la organización interna son el basamento para resolver las problemáticas actuales.

Pues, la no participación de la provincia de Entre Ríos en la Comisión de Trabajo y, en consecuencia, el Plan de Acción, no es óbice para considerar los Lineamientos referenciados como un norte propicio y necesario para adaptar los procedimientos afines locales a la era digital y la maximización de la protección de datos puertas adentro de la Administración.

1.1.- <u>(In) suficiencia de los mecanismos de contralor y fiscalización administrativos para el correcto manipuleo de los datos y del "Big Data".</u>

Sin lugar a duda, los mecanismos de contralor propios de la Administración -tanto previo como posterior al obrar administrativo-tienen como finalidad el logro de la eficiencia y el actuar conforme a derecho, ello en el marco del principio de legalidad. Es allí donde radica la importancia de la fiscalización de los actos administrativos, máxime en aquellos campos en los que se cuenta con margen de discrecionalidad.

Particularmente, en el presente trabajo de investigación, cobra relevancia el control preventivo no solo de los actos sino también del comportamiento del Estado frente a la tutela de los derechos a la protección de datos y a la dignidad, en pos de la intimidad y la vida privada.

Si bien una legislación nacional o local nunca será suficiente para regular la debida recopilación de datos de manera transversal, sí es cierto que el Estado -en todos sus estamentos- participa de una u otra manera en el entramado de las reglas de juego relativas a los datos personales.

Ello así, los anteproyectos de reforma de la Ley de Protección de Datos Personales prevén su redacción en pos de los nuevos criterios vigentes en Europa.[37] En consonancia con ello, el Reglamento General de Protección de Datos de la Unión Europea, recientemente reformado, incorpora nuevos principios tales como el de responsabilidad "*accountability*", en tanto manda implementar mecanismos que permitan acreditar que se han adoptado las medidas necesarias para tratar los datos personales conforme exige la norma (responsabilidad proactiva); en parte lo que se propone en el presente trabajo.

En cuanto al control de su aplicación, el Reglamento Europeo establece que los organismos de control deben ser públicos, independientes y cooperar entre sí y con la UE, sus funciones son más amplias que la sola aplicación del reglamento, por ejemplo, tienen la responsabilidad de sensibilizar al público y empresas respecto de la temática, brindar información a interesados y estar pendiente de los cambios tecnológicos que puedan afectar la protección de datos. La norma, además, crea un Comité Europeo de Protección de Datos, de carácter supranacional, cuya función es controlar a las autoridades de control de cada Estado.

[37]Ley de Protección de los Datos Personales en Argentina. Sugerencias y aportes recibidos en el proceso de reflexión sobre la necesidad de su reforma. Agosto – diciembre 2016. Dirección Nacional de Protección de Datos Personales. https://www.argentina.gob.ar/sites/default/files/documento_aportes_reforma_ley25326_0.pdf

Otro eje en el que la normativa europea ahonda refiere a cómo y con qué criterios deben tratarse los datos. En su artículo 5, plantea que el tratamiento debe ser lícito, leal y transparente para con el interesado, adecuado, pertinente y limitado a los fines para los cuales fueron relevados (que deben estar previamente determinados, ser explícitos y legítimos). Los datos deben ser además exactos y estar actualizados, y su plazo de conservación debe limitarse a la función para la cual fueron recolectados. También debe garantizarse que no sean accesibles a un número indeterminado de personas. El responsable de su tratamiento debe ser capaz de demostrar todo esto y tiene la obligación de responder a las consultas de las autoridades de control y de los interesados.

Además, el tratante de los datos debe evaluar, previamente a su utilización, el impacto que ésta podría tener para los derechos y libertades de los titulares. En caso de violación de la seguridad de los datos durante el proceso, debe notificarlo a la autoridad de control y al interesado.

En efecto, si bien los anteproyectos referenciados *ut supra* actualizan la norma del año 2000 e introducen algunos avances -como la responsabilidad de los tratantes de datos de realizar una evaluación de impacto previa a su utilización o el derecho de toda persona a interponer acción de amparo, sin que necesariamente exista un motivo de sospecha de incumplimiento demostrable-, su texto nuevamente presenta más excepciones que reglas, y muchas de esas excepciones son aplicables al uso que, de los datos, efectúa el Estado.

Ciertamente, en el compilado de aportes y sugerencias previo a la redacción del proyecto de reforma a la ley, los actores convocados eran coincidentes en que -bajo el amparo de la ley vigente- el Estado detenta demasiadas prerrogativas en lo que hace al manejo de los datos personales de los particulares y que debe expandirse la capacidad de la Dirección Nacional de Protección de Datos -en adelante DNPDP- para cumplir con sus deberes de contralor, aumentando su autonomía y financiamiento. Asimismo, insistieron en la necesidad de dotar de la figura de "delegados" de la DNPDP dentro del sector público, a los efectos de controlar el cumplimiento del deber de confidencialidad y protección de los estándares.

Puntualmente, en lo que respecta al tratamiento de datos por organismos públicos, la coincidencia fue plena en torno a que las garantías previstas en la normativa actual no son aplicables a las bases de datos estatales, por lo que el Estado seguiría contando con una

excesiva permisividad de almacenar, tratar y ceder datos personales; por lo que enfatizaron en la necesidad acuciante de incluir una limitación de las capacidades del Estado para realizar operaciones con datos personales.

Entre las sugerencias se soslayó el requisito del consentimiento o del interés legítimo, adicionando que el Estado deba cumplimentar con los demás principios del sistema, en particular del principio de finalidad, de adecuación y pertinencia de datos; como así también de activar mecanismos que desmotivaran al funcionario del uso de ciertas bases de datos personales para finalidades que estuvieran por fuera su competencia. Incluso, una de las Asociaciones de la sociedad civil consultadas -Fundación Vía Libre- referenció que la normativa actual establece una serie de flexibilidades y excepciones que desprotegen a los ciudadanos frente al Estado y al sector privado, especialmente, de cara al sector de la economía de la información que tiene, en los datos personales, el insumo fundamental de su negocio.

Puede evidenciarse que, en los proyectos de reforma de la ley se incorpora el principio de responsabilidad proactiva -en torno a la importancia de la tenencia responsable del dato y las medidas que se toman para lograrlo-; y el interés legítimo como una excepción al consentimiento -el que no será válido en caso de tratamiento de datos por autoridades públicas-. A ello debe añadirse que nada dicen respecto a los metadatos o "Big Data", ergo datos sobre datos: información estructurada que describe a otra información, de suma utilidad para estadísticas e implementación de políticas públicas.

La importancia de los metadatos radica en que permiten revelar tanto o más acerca de las personas que el propio contenido de las comunicaciones, ya que a través de ellos se pueden establecer patrones de comportamiento, hábitos o relaciones. A la fecha no se ha dado nuevo tratamiento al proyecto, pese a la imperiosa necesidad de adaptar la normativa a la realidad circundante.

La normativa actual prevé la creación de un órgano de control, dotado de capacidad para llevar a cabo las acciones necesarias para el objetivo y fines de la ley, a saber: "DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES" (DNPDP); con competencias concretas tales como asistir y asesorar en torno a los alcances de la normativa y los medios legales de protección, dictar la reglamentación para el desarrollo de

las actividades propias de la norma, controlar la observancia sobre integridad y seguridad de datos, imponer sanciones administrativas por violación a la ley.

Incluso, la ley prevé que dicho órgano de control estará compuesto por un/a Director/a que contará con dedicación exclusiva y alcanzado por las incompatibilidades de los funcionarios públicos, solo pudiendo ser removido por el Poder Ejecutivo por mal desempeño.

Es de desatacar que dicho órgano de control se ha desempeñado prácticamente fiscalizando la observancia de las normas por particulares, personas jurídicas, y empresas privadas; mas no así en torno al proceder del propio Estado puertas adentro; el que encuentra un ámbito de actuación con amplia discrecionalidad. A mayor abundamiento puede destacarse que, conforme información de acceso público brindada por la Asociación de Derechos Civiles, las inspecciones realizadas por la DNPDP han sido todas a empresas privadas, nunca a una dependencia estatal. Es posible verificar, en el análisis de las sanciones por violación de la ley impuestas por la DNPDP quelas 36 sanciones aplicadas por la DNPDP entre 2005 y 2013 fueron impuestas a entidades privadas. (Asociación por Derechos Civiles 2014).

Dicho organismo fue vetado por falta de previsión presupuestaria. Un año después, se creó la Dirección Nacional de Datos Personales en el Ministerio de Justicia y Derechos Humanos, como autoridad de aplicación, con un/a Director/a designado por el Poder Ejecutivo. En el año 2016, a través de la ley 27.275 se creó la Agencia de Acceso a la información Pública que paso a depender de la Jefatura de Gabinete de Ministros, como organismo de control de esa norma y de la Ley de Protección de Datos Personales. Actualmente, a nivel nacional, la autoridad de aplicación es el Jefe de Gabinete de Ministros, lo que dista mucho del organismo de contralor descentralizado creado por ley. No existe, claramente, independencia y autonomía en el órgano de control.

Recientemente, en el ámbito Nacional se dictó la Decisión Administrativa DECAD-2021-641-APN-JGM[38], que prevé los requisitos mínimos de Seguridad de la Información para Organismos del sector público nacional y ordena a las entidades y jurisdicciones del Sector Público Nacional enmarcados en la Administración Financiera y de Control (Ley N°

[38]https://www.boletinoficial.gob.ar/detalleAviso/primera/246104/20210628

24.156)a aprobar sus Planes de Seguridad. Sus objetivos específicos se presentan como: proteger los derechos de los titulares de datos personales o propietarios de información que es tratada por el Sector Público Nacional, proteger la información, los datos personales y activos de información propios del conjunto de organismos que componen el Sector Público Nacional, promover una política pública que enmarque una conducta responsable en materia de seguridad de la información de los organismos que conforman el Sector Público Nacional, sus agentes y funcionarios, evidenciar el compromiso e interés de quienes componen el Sector Público Nacional en pos del desarrollo de una cultura de ciber seguridad.

Conforme se especificó al inicio del presente trabajo, la provincia de Entre Ríos no ha adherido a la Ley de Protección de Datos, por lo que actualmente la normativa aplicable se vincula directamente con los estándares internacionales ya referenciados; el Art. 43 de la Constitución Nacional y el Art. 13 de la Constitución Provincial que refiere a las herramientas legales para la protección y tutela de la información respectiva a las personas que vulnere su honra y honor. No existe, en consecuencia, organismo específico de contralor y fiscalización a nivel local en torno a la protección de datos personales, menos aún una reglamentación interna afín.

Ello refleja que, a nivel local no existe un mandato de control de oficio sobre la cuestión, ni un organismo concreto dotado de las competencias para tal fin. En efecto, el control es posterior, desde el individuo y cuando el daño ya se ha concretizado. Ciertamente, el reclamo es judicial, por cuanto la herramienta por excelencia es el amparo. La situación de extrema vulnerabilidad de la ciudadanía frente a la temática obliga a repensar la imperiosa necesidad de establecer un mecanismo de contralor, con más una organización interna de la Administración que impetre por la protección de datos personales de carácter preventivo.

Consecuentemente, transitado el contacto del dato con el operador administrativo y los organismos respectivos; no existe localmente un órgano específico y creado al efecto -*ad hoc*- cuyo objeto determinado sea controlar el cumplimiento de los principios rectores de la ley de protección de datos, léase: confidencialidad, tutela a la integridad y vida privada y no divulgación. En otras palabras, el dato ingresa y no reviste mayor tutela preventiva que la implícita de cada operador por su propia convicción y conocimiento en la materia y la pro actividad del ciudadano que brinda la información en requerir, ante la constatación de un uso

indebido, su protección. El único mecanismo de tutela vigente es el recurso de Habeas Data, como un accionar del particular ante el quebrantamiento ya acontecido.

Un reciente estudio (2015) publicado en el Simposio Argentino de Informática y Derecho, titulado "Principios Nacionales e Internacionales en el marco de la Protección de Datos Personales. Deficiencias. Recomendaciones"[39], analizó si nuestro país poseía legislación eficiente a la hora de proteger los derechos a la privacidad e intimidad. Sin perjuicio de analizar detalladamente las marcadas excepciones a la regla que la normativa -hoy vigente- detenta, hizo asimismo hincapié en la importancia de la provisión al ciudadano de información acerca de la localización y quien ha obtenido datos de su persona, ello por cuanto deviene un elemento fundamental para ejercer la autodeterminación informativa y los debidos derechos de tutela.

Ciertamente, concluyó que el ejercicio de los derechos de tutela por parte del titular de los datos depende de la discrecionalidad del responsable que los recabo y los posee bajo el amparo de la normativa imperante, recomendando fuertemente no solo lograr un tratamiento igualitario respecto de las bases públicas y privadas -remarcando la necesidad de control sobre las bases públicas-; sino también impetrando la conformación de una autoridad competente, independiente e imparcial para ejercer un real control sobre las bases de datos, con énfasis en la supervisión publica de intervención de los ciudadanos.

En un contexto de marea de información y de insuficiencia de legislación local en torno a la debida organización y procedimiento a estructurar para el funcionamiento del sistema de control de protección de datos, pero evidenciando que existe un conjunto de normas y principios que traspasan los nacional y afectan a todos los sistemas jurídicos, deviene imperioso traer a colación el planteamiento teórico de REYNA en el estudio del derecho administrativo multidimensional; mediante el cual propone una reforma de la Administración con basamento en un régimen jurídico especial de armonización y construcción desde abajo hacia arriba, ergo partiendo desde el caso concreto para la construcción de un sistema específico que tutele la situación jurídica subjetiva que afecta al individuo.

[39] http://sedici.unlp.edu.ar/bitstream/handle/10915/58627/Documento_completo.pdf?sequence=1

Propone la aplicación de una red transversal de las distintas dimensiones jurídicas para solucionar el caso.

En el caso en estudio, que tiene en miras indagar acerca de los límites de la Administración local para la protección de los datos de las personas; y la evidente ausencia de una reglamentación especifica en la provincia sobre la materia; resulta interesante pensar en construir un proceso organizativo que resuelva el caso concreto internalizando los distintos sistemas jurídicos, nacionales e internacionales, en pos de arribar a un esquema de organización que permita brindar soluciones al ciudadano, con basamento en la tutela de los derechos fundamentales e incluyendo, incluso, mecanismos organizativos importados del derecho privado en torno al concepto de responsabilidad social.

Sin duda se presenta el cuestionamiento de las competencias (materiales y territoriales) para obrar, y la necesidad que ese actuar articulado provenga de un acuerdo tácito de los distintos estamentos, ergo la dificultad de llevar a la praxis la dogmática.

Ahora bien, en correlato a lo expuesto en los párrafos precedentes, puede sí pensarse en una reforma de la Administración hacia adentro, adaptada a las nuevas realidades circundantes y que sí considere los mecanismos de contralor como parte integrante de los procesos organizativos, lo que REYNA ha llamado el "método aplicable a las organizaciones administrativas"; que deja de lado las jerarquías para establecer mecanismos de dirección basados en un orden material de valores, cuyo origen emerge de la constitución nacional.

Resulta innegable que actualmente se cuenta, por decir lo menos, con una guía legislativa internacional que plantea las pautas y directrices en torno al debido comportamiento de los Estados -puertas adentro-, en relación con la temática en estudio.

En otras palabras, las herramientas existen, y se encuentran al alcance del legislador, por lo que el eje central deben ser los derechos fundamentales y las prácticas adecuadas, sin temor a la aplicabilidad de experiencia de otros países.

Conforme lo refiere el Comité Jurídico Internacional de la OEA en su Informe del año 2015: "…se insta a los Estados Miembros a que establezcan disposiciones, procedimientos o instituciones jurídicos, administrativos y de otros tipos que sean apropiados y eficaces para proteger la privacidad y las libertades individuales con respecto a los datos personales. Deben crear medios razonables para que las personas ejerzan sus

derechos y fomentar y apoyar la autorregulación (con códigos de conducta o por otros medios) de los controladores de datos y los procesadores de datos. Asimismo, deben establecer sanciones y recursos adecuados para los casos de incumplimiento y cerciorarse de que no se discrimine injustamente contra los titulares de los datos".

Dicho esto, la propuesta se basa y enfatiza en la armonización normativa, en conjunción con la creación de organismos de control y fiscalización eficientes, competentes y, sobre todo, independientes, que propendan a una efectivo y adecuado tratamiento de los datos personales por parte del Estado; sea mediante los mecanismos que fueran -lícitos claro está-, que permitan incorporar dentro de los procesos de recopilación masiva de datos por la Administración, el debido control y enfoque en la responsabilidad, protección y tutela de los derechos fundamentales.

Ciertamente, la necesidad de una efectiva autoridad de control en materia protección de datos personales radica en la posibilidad de contar con un derecho de los titulares a tener control sobre los mismos. Esto es así, entre otras razones, por la inexistencia de un ente fiscalizador, de un procedimiento administrativo de reclamo, y la falta de sanciones eficaces y disuasivas. No puede negarse que el mundo moderno se estructura en base al uso de la información, y la masividad de información reclama un organismo de control.

1.2.- El Estado de Bienestar Digital como imperativo para la Sociedad Digital.

Lo antedicho obliga a mirar al usuario -ciudadano-, observarlo y pensarlo en pos de una reingeniería del proceso, ello para una mejora en el acceso a los servicios públicos, poniendo énfasis en conjugar la erradicación del trámite eterno, implementando las nuevas formas de comunicación e interacción con las personas. La cuarta revolución industrial caracterizada por la tecnología, lo digital y la robótica, la internet de las cosas y el *big data*, con más la implementación de las TICs[40] para la eficiencia en servicios interpela a pensar y analizar si la sociedad actual, local, se encuentra a la altura de las circunstancias.

En efecto, el grado de digitalización local reclama -aun así sea marcadamente menor a los países europeos y norte americanos- corroborar si la brecha digital entre el crecimiento y avance tecnológico y el efectivo acceso de los ciudadanos a dichos servicios ha sido

[40]Tecnologías de la Información y Comunicación como herramientas para el proceso, administración, y distribución de información a través de elementos tecnológicos.

superada. La incorporación de principios del sector privado a la gobernanza, como la calidad, eficiencia y atención al cliente han generado una nueva forma de gobernanza de bienestar, cambios claro está acompañados por la tecnología. El gobierno electrónico da por sentado la accesibilidad plena, pero en los países emergentes y en desarrollo, se complejiza una estandarización del Estado de Bienestar Digital.

Sin perjuicio de ello, y las facilidades de transformación que conlleva la digitalización de los procesos, tales como su agilización y transparencia, y en relación con el trabajo en estudio, no puede obviarse que el efectivo acceso al nuevo gobierno reclama no solo la "accesibilidad" antedicha, generando una brecha inescindible sobre la población de mayor vulnerabilidad e imposibilitada de digitalizar su vida diaria, sino también considerando que quienes acceden, suscriben la incorporación de datos e información personal de manera irrestricta, lo que peligra la tutela de los derechos fundamentales y reclama un análisis a conciencia.

Es por ello que, al pensarse en gobierno electrónico no solo debe estarse a la garantía del acceso a la infraestructura y servicios digitales para toda la población, sin discriminación, sino también en la concreción de un efectivo procedimiento de contralor y tutela para la protección de la vida privada de las personas, con el objeto de evitar que la entrega masiva de datos sin control se transforme en una fuga de información personal sin restricciones.

No debemos obviar la importancia y preponderancia que receptan, en la sociedad digital, el valor económico de los datos y el reconocimiento social de los algoritmos, principalmente aquellos que se encargan del procesamiento de datos y; que ello conlleva, en muchos casos, un uso irrestricto de las herramientas al alcance.

Pensemos, a modo ejemplificativo, el Big Data en el campo sanitario; en otras palabras, la acumulación masiva de datos relativos a la salud de los individuos que permite el acceso a un gran volumen de datos y con excesiva rapidez. Justamente, por el volumen y la masividad, en conjunción con la facilidad de acceso -por cuanto es el propio ciudadano el que aporta la información para acceder al servicio, vgr. vacunación- se genera un mayor riesgo para el derecho a la privacidad o, en su caso, la recientemente reglamentada 'historia clínica electrónica' y creación del Programa Federal Único de Informatización y Digitalización de Historias Clínicas de la República Argentina (Ley Nº 27.706 y Dec. 393/2023). Ello así, deben reforzarse las garantías jurídicas de protección, máxime cuando

el recolector de los datos es el propio Estado, en esta vinculación inescindible e inevitable con la que se encuentra el ciudadano para acceder a los servicios básicos y el Estado para proporcionarlos.

Cierto es que, el presente estudio busca indagar los limites existentes en la Administración local -provincial- en torno al debido uso y tratamiento de los datos personales que el ciudadano proporciona al Estado para la realización de sus fines; ello enmarcado en el vínculo inescindible Estado-Sociedad y transversalmente por todos los organismos.

Ahora bien, la realidad de la existencia de distintos estamentos (comunas, municipios, provincias y nación); y sus respectivos ordenamientos jurídicos y administrativos; no puede dejar de lado que los actos administrativos que de ellos emanan deben tener un común denominador basado en la norma fundamental, pues ciertamente cualquier decisorio en contra de nuestra Carta Magna va en detrimento del esquema normativo primigenio que atraviesa todo el territorio y es el basamento de un Estado de Derecho Constitucional.

Dicho esto, pues debe existir cierta unidad de ordenamiento en los distintos estamentos, máxime cuando se trata de tutelar derechos fundamentales. Consecuentemente, en el tema que nos ocupa y que impetra por crear una organización local que prevea la tutela referenciada vinculada a los datos personales, debe partirse de la concepción de incertidumbre frente a los nuevos retos de la gobernanza electrónica para, de esta manera, propender a la búsqueda de alternativas y soluciones que disten de las ya conocidas y aplicadas.

Los principios rectores fundamentales en la materia, de autodeterminación informativa y responsabilidad proactiva, debieran ser los pilares fundamentales para la coordinación de procesos de protección desde el Estado al ciudadano. Deben ser el núcleo medular que adopten los distintos organismos para aplicar una efectiva tutela de los datos a los que se accede. En efecto, conforme se ha especificado en los párrafos precedentes, en la sociedad informatizada se ha iniciado un movimiento -sobre todo en la doctrina y jurisprudencia más avanzada de los países con alto grado de desarrollo tecnológico-, tendiente al reconocimiento de la libertad informativa, es decir la facultad de autodeterminación y al procesamiento automatizado de datos de carácter personal.

En la era de la sociedad digital o sociedad de la información es innegable que el camino apunta hacia la creación de nuevas formas de administración, guiadas por las plataformas tecnológicas de fácil acceso y de celeridad en los procedimientos, incluso al punto de la toma de decisiones a través de herramientas de inteligencia artificial por el uso de algoritmos. Dichos acelerados avances ya en aplicación, y cuyo funcionamiento se nutre ineludiblemente de los datos que proporciona -a sabiendas o no- el ciudadano de a pie; deben tener como correlato la debida aplicación de pautas conductuales, códigos de ética y principios comunes y afines que eviten un uso extralimitado de los datos.

La solución debiera ser preventiva, en conjunto con el armado del Estado Digital, y no como soluciones particulares ante el caso concreto (como problema), muchas veces judicializado.

Actualmente, las herramientas se encuentran al alcance, por cuanto las pautas directrices de cómo debe comportarse el Estado frente a estas situaciones se encuentran ya plasmadas en instrumentos internacionales que componen el *SoftLaw internacional*, con más los principios rectores, a lo que debe adicionarse la experiencia internacional en la temática, y cómo la inconducta de los Estados en la protección de los datos personales se puede ver reflejada en reclamos de particulares que pueden echar por tierra políticas públicas que, en su caso, podrían tener fines beneficiosos.

En efecto, la importancia radica en el cómo se implementan estas nuevas herramientas, en la cautela de salvaguardar derechos fundamentales para evitar enfrentarnos a frenos y contrapesos por un uso inadecuado y deliberado de los datos, consecuencia del desconocimiento.

Ciertamente, cabe referenciar que las limitaciones que deben imponerse al tratamiento y uso de los datos personales por parte de la Administración lo son con la efectiva intención de proteger este derecho fundamental y, asimismo, su vocación internacional con claras incidencias en los vínculos estatales.

Frente a ello, podría a estarse a un ámbito de colaboración recíproca entre el derecho público y el privado, conforme se propusiera *supra*; ello en torno a comprender que el sector privado desarrolla actividades estratégicas y de interés general vinculadas a la proliferación de datos -vgr. telecomunicaciones, plataformas, Apps, entre otros-, en donde ya existen

ordenamientos normativos propios, de autorregulación, no solo como estándares o reglas de calidad, sino también como evaluación del impacto social y para evitar riesgos que, en definitiva, pudieran llegar a afectar el sistema productivo particular.

Otro factor fundamental e ineludible de estos nuevos procesos es justamente el papel asumido por la sociedad frente a estas nuevas realidades digitales. La vida de los particulares se ha intensificado y los espacios se han diversificado, por lo que las políticas públicas y de organización deben tener en cuenta todos los escenarios de actuación.

La globalización, que trajo consigo la Sociedad Digital, impetra por una transformación estatal tanto hacia adentro como hacia afuera, entendida esta última como el espacio exterior considerado en la actuación comunitaria de la Administración. Todos estos desplazamientos tienden a virar el rumbo regulatorio, en miras de generar y tender redes que entrecrucen ordenamientos, para hallar la solución más adecuada y nuevas formas de organización.

Sin dudas, se vuelve al esquema ya planteado y tan necesario: procedimiento y organización administrativa para la tutela de los derechos fundamentales, por cuanto deciden el modo de ser y de decidir de la Administración, y otorgan eficacia y transparencia a las conductas del Estado Digital.

No puede desoírse que, en la sociedad contemporánea "sociedad de la información" la intimidad ha perdido su carácter exclusivo individual y privado, para asumir progresivamente una significación publica y colectiva, producto del cauce tecnológico y, consecuentemente, ha ido migrando desde un sentido estático de defensa de la vida privada a una función dinámica de controlar la circulación de información relevante para cada sujeto, en otras palabras: el control que tenemos sobre la información que nos concierne.

Resulta insuficiente hoy concebir a la intimidad como un derecho garantista de defensa frente a cualquier invasión indebida en la esfera de la vida privada, sin contemplarla al mismo tiempo como un derecho activo de control sobre el flujo de información que afecta a cada sujeto. Por ello, es que se reclaman mecanismos de control que puedan hacer frente a su uso y manejo.

Sumado a lo expuesto, en el actual Estado tecnológico ya no solo entran en juego intereses individuales -de tutela vs. principio de finalidad-, sino también intereses colectivos,

para evitar injerencias arbitrarias de carácter tecnológico, tales como las políticas de video vigilancia como campo de acción del Estado para garantizar la seguridad pública. En efecto, un estudio sobre el estado de la legislación sobre video vigilancia en Argentina ha concluido que, como las condiciones para la licitud de la aplicación de sistemas de monitoreo están presentes en forma dispar en las leyes provinciales, sin que haya una vulneración directa de derechos, tampoco se puede afirmar que haya una completa armonía entre los sistemas de video vigilancia (y su fin de brindar seguridad) con los derechos a la imagen, privacidad e intimidad[41].

En relación con ello, huelga traer a colación la sentencia 14/2003 del Tribunal Constitucional Español[42], que refiere a la publicación de cuerpo entero de la fotografía de una persona que se presenta voluntariamente a la policía para aclarar la participación en un hecho de violencia. La policía, además de tomarle declaración le saca una fotografía y la publica en diferentes medios. El denunciante se presenta, contra el Estado, reclamando por el derecho al honor, privacidad e imagen. El Tribunal entiende que, para considerar si una medida es restrictiva de un derecho fundamental es necesario constatar si cumple tres requisitos: si la medida es susceptible de conseguir el objetivo propuesto (idoneidad), si es una medida necesaria en tanto no exista otra más moderada (necesidad) y si es equilibrada (proporcionalidad). En definitiva, el Tribunal considera la fotografía como un dato de carácter personal, obtenida y captada por las fuerzas policiales del Estado en el ejercicio de su función constitucional, respecto dela cual sus miembros están obligados al secreto profesional así, "*La constitucionalidad de cualquier medida restrictiva de derechos fundamentales viene determinada por la estricta observancia del principio de proporcionalidad*" (SSTC 66/1995, 186/2000) [FJ 9].

En efecto, a través de la historia hay sobrados ejemplos de que "Los datos de las personas no solo se han recopilado con fines estadísticos, han sido recopilados con fines de control, sobre todo en los regímenes autoritarios; se han utilizado como instrumento de discriminación, marginación y segregación."[43] Sin perjuicio de ello, también los Estados

[41]CEJAS, EILEEN BERENICE Y GONZÁLEZ, CARLOS CÉSAR. "Estado de la normativa sobre video vigilancia en Argentina y su relación con la protección de datos personales". SID 2015, 15º Simposio Argentino de Informática y Derecho. adfa, p. 1, 2011. © Springer-Verlag Berlin Heidelberg 2011.

[42] STC Español 14/2003. 28.01.2003.

[43]Víctor Abramovich y Christian Courtis, "La aplicación de los Tratados Internacionales sobre DD.HH por los Tribunales Locales" pág.299 en ROMERO SILVERA, GRACIELA. "Interés público y protección de datos personales con especial referencia a los Derechos Humanos". SEMINARIO REGIONAL DE PROTECCION DE DATOS. Montevideo, Uruguay, 1- 4 de junio de 2010.

están obligados a instrumentar medidas adecuadas para garantizar y proteger los derechos de todas las personas, habilitando la guarda de datos sensibles para fines determinados fundados en razones de interés colectivo, vgr. salud pública, orden público, defensa, entre otros; siempre y cuando ello se encuentre así especificado en una ley.

Para el caso particular, se ha abordado un trabajo investigativo publicado por Luis Ordoñez Piñeda[44], que analiza y estudia los precedentes del origen y desarrollo del derecho a la protección de datos personales en la comunidad andina, para promover un modelo interamericano de integración con el objeto de una regulación equilibrada respecto al tratamiento de los datos personales.

Para ello, parte de la base de la consideración del derecho referenciado como un derecho autónomo y constitucionalmente tutelado, como así también que el sistema latinoamericano de tutela debiera asemejarse al europeo -cuya virtud ha sido universalizar principios y criterios jurídicos para brindar un marco homogéneo de regulación-, ello con basamento en un creciente proceso de transformación y de dispersión normativa en la región.

Finalmente, en lo que respecta a definiciones jurisprudenciales, el autor trae a colación lo resuelto por la Corte Suprema de Justicia de Argentina mediante sentencia XXXlll, sobre la cual no refiere mayores datos de identificación para su lectura íntegra, y cita, a saber: "*La protección legal se dirige a que el particular interesado tenga la posibilidad de controlar la veracidad de la información y el uso que de ella se haga. En tal sentido, este derecho forma parte de la vida privada y se trata, como el honor y la propia imagen, de uno de los bienes que integran la personalidad. El señorío del hombre sobre sí se extiende a los datos sobre sus hábitos y costumbres, su sistema de valores y de creencias, su patrimonio, sus relaciones familiares, económicas y sociales, respecto de todo lo cual tiene derecho a la autodeterminación informativa (...) A esta decisión se le atribuye la configuración del concepto de "autodeterminación informativa" o libertad informática, que es reconocido actualmente en forma predominante como el fundamento del hábeas data en las legislaciones que contemplan derechos análogos [...] Según este concepto* ***es el ciudadano quien debe decidir sobre la cesión y uso de sus datos personales****. Este derecho -se dijo-****puede ser restringido por medio de una ley por razones de utilidad social, pero respetando el***

[44] ORDOÑEZ PIÑEDA, LUIS. "La protección de datos personales en los estados que conforman la Comunidad Andina: estudio comparado y precisiones para un modelo interamericano de integración". Revista de Derecho, No. 27, ISSN 1390-2466 • UASB-E / CEN • Quito, 2017.

principio de proporcionalidad y garantizando que no se produzca la vulneración del derecho a la personalidad". (el resaltado me pertenece).

El estudio concluye ratificando acerca de la necesidad de buscar un equilibrio entre la Administración y los ciudadanos, como un pacto social que garantice la proporcionalidad de las libertades, para lo cual es necesario un adecuado ordenamiento jurídico, proponiendo, en consecuencia, un reglamento interamericano que impida dispersión normativa y compatible con los instrumentos internacionales, y la adopción de medidas legislativas internas y políticas sectoriales que aseguren el derecho a la autodeterminación informativa y su defensa, mediante la creación de autoridades de control.

La utilización de la tecnología de la información por parte del Estado, sin posibilidad de control alguno del ciudadano, puede afectar su privacidad e intimidad; generando un poder sin límites sobre el individuo, mediante la prerrogativa de acumular bases de datos personales y procesarlos para generar patrones de conducta y perfiles personales, generándose un contrapeso a través del desarrollo normativo del derecho a autodeterminación informativa.

Ahora bien, conforme se ha detallado en el presente trabajo, pues la implementación de legislación acorde para combatir toda intromisión en la esfera privada de las personas no resulta suficiente, siendo necesarias políticas públicas concretas por parte de los Estados y un esquema organizativo de control hacia adentro, máxime advirtiendo que el estrepitoso ritmo de avance de la tecnología de la información y comunicación (TICs) resulta inalcanzable para el derecho actual.

No es un dato menor que la mayor acumulación de datos personales se da en los organismos descentralizados y centralizados de la Administración Pública, radicando la mayor ineficiencia en la carencia de independencia de los organismos de control, por demás inexistente en la provincia de Entre Ríos.

Una alternativa, propuesta por el Dr. Carlos Eduardo Saltor en su tesis doctoral referida a un estudio comparado de la protección de datos[45], es la utilización -provisoria- de la figura del Defensor del Pueblo jurisdiccional, dotándolo de competencias al efecto, a lo que debe adicionarse un factor preponderante; esto es el aprendizaje tanto de la

[45]SALTOR, CARLOS EDUARDO. "La Protección De Datos Personales: Estudio Comparativo Europa-América Con Especial Análisis De La Situación Argentina". memoria para optar al grado de doctor. Madrid, 2013.

Administración como de los administrados, en torno a la efectiva tutela de este derecho fundamental, brindando información, campañas de concientización y fomentando el control personal, estableciendo asimismo procesos fáciles de acceso y rectificación por parte de la ciudadanía, extrajudiciales claro está.

Conforme se detallará en los capítulos siguientes, las múltiples alternativas son diversas, y no puede tildarse cuál es más adecuada sino teniendo en consideración no solo el contexto social y político de cada Estado, con más sus vinculaciones en el plano internacional, sino por cuanto -asimismo- deviene innegable que la casuística aún no ha atravesado un margen temporal de apreciación que permita extraer conclusiones adecuadas acerca del mecanismo más certero; siendo que asistimos no solo a un derecho en formación, sino a mecanismos y procedimientos nacientes en forma concomitante con la sociedad digital, en constante y dinámico cambio.

CAPÍTULO II: ESCENARIO INTERNACIONAL EN TORNO A LA PROTECCIÓN DE DATOS PERSONALES FRENTE A LA ADMINISTRACIÓN PÚBLICA LOCAL Y GLOBAL.

2.1- Estándares internacionales para la protección de datos personales. Impacto del avance de la Era Digital aplicada a la Administración Pública.

Ya me he referido al inicio del presente trabajo acerca de las fuentes del derecho administrativo, temática que hoy ha cobrado relevancia en tanto el derecho internacional –en constante transformación- ha impactado en el derecho interno generando sendos cambios en la concepción de la efectiva creación normativa y el carácter del *SoftLaw* internacional, de la mano de la globalización.

Lo referenciado en el párrafo precedente se encuentra en estrecha vinculación, o mejor dicho haya su basamento, en las nuevas situaciones o fenómenos que se presentan en el plano internacional y que se avizoran en lo local, todo lo cual reclama un debido tratamiento jurídico. Actualmente, no puede pensarse el mundo del derecho en general y, claro, del derecho administrativo en particular escindido de los derechos humanos

consagrados internacionalmente y de los múltiples organismos internacionales de tutela, como así también las agencias, organizaciones e instituciones globales que crean normas vinculadas a los comportamientos de los Estados, tanto como garantes de derechos fundamentales como de hacedores del buen gobierno.

Entonces, no escapa a este trabajo el fenómeno de gestación de nuevos procesos de creación normativa, mucho más amplios, blandos y flexibles: el denominado *SoftLaw* internacional, como una nueva manera de pensar y crear el derecho, ello desde una perspectiva de reglas internacionales con incidencia en los derechos internos posicionando a la persona humana como eje central y virando la concepción del ordenamiento jurídico.

A decir de Villar Palasi, y reiterando lo ya referenciado, rompiendo el concepto de norma completa en tanto se presenta como los 'elementos desgajados' del ordenamiento jurídico, aplicando los elementos dispersos de la norma desde el caso concreto, siendo el operador quien debe buscar la norma y sus elementos para aplicar al caso. Ello así, al arribar a la solución 'justa', se genera un grupo normativo aplicable al caso concreto, normas que han sido seleccionadas y obtenidas del derecho blando al efecto para garantizar la mejor respuesta posible.

En ese sentido, la categorización de dichas normas de derecho 'blando' e históricamente atendidas como fuentes materiales ha ido perdiendo espacio, en tanto su existencia autónoma ha marcado reglas de conducta de los Estados (producto de un arduo proceso evolutivo de consenso) cuyo incumplimiento hoy es impensado, al punto de obrar fuera de toda discusión su obligatoriedad en tanto operan como códigos de conducta formales con consecuencias jurídicas, que bregan por arribar a soluciones justas para casos concretos -dotadas de mayor consenso a nivel internacional-.

Párrafo aparte merece la cuestión de la exigibilidad, lo que no opaca el marcado cumplimiento espontaneo que se advierte en la comunidad global para adquirir confianza y credibilidad ante los actores internacionales, y ha puesto en jaque su consideración de fuente material o formal de derecho.

Lo antedicho busca reforzar el entendimiento de la importancia de una debida incorporación al derecho administrativo local de reglas de conducta propias de los Estados producto del consenso internacional, y la consecuente toma de decisiones vinculada a dichos

estándares -en el caso- para la protección de datos personales. Dichos mandatos de optimización deben ser interpretados a nivel local en procura de una mayor y mejor protección de los derechos.

Ello así, la nueva gobernanza vinculada a la sociedad de la información reclama alternativas a las formas de gobierno tradicional, con el fin de orientar las políticas públicas de manera más eficaz, garantizando no solo que los efectos de la toma de decisiones se basen en el debido respeto a los derechos humanos; sino también en que los procesos y procedimientos internos de las Administraciones Publicas resguarden la tutela del ser humano como individuo.

Entonces, en el análisis de la protección de datos personales en el seno de la administración pública local no solo se interpela la organización administrativa, sino también la especial relación del individuo con el Estado, que deben regirse por el ordenamiento jurídico local pero supeditado a las reglas conductuales establecidas en el ordenamiento global. Se presentan, de esta manera, como dos campos que ya no pueden escindirse y deben ser tenidos en cuenta al momento de las múltiples vinculaciones y accionar del Estado que afecten al ciudadano y, en particular, sus datos personales.

Oportunamente, al inicio del presente trabajo, se especificaron concretamente los estándares internacionales referidos a la protección de datos personales como normas que garantizan un nivel mínimo de protección; entre lo que se pueden enumerar: el nuevo Reglamento (UE) 2016/679 del PARLAMENTO EUROPEO y del CONSEJO del 27 de abril de 2016, los Estándares de Protección de Datos Personales para los Estados Iberoamericanos establecidos en el marco del XV Encuentro Iberoamericano de Protección de Datos de la Red Iberoamericana de Protección de Datos, el Informe del Comité Jurídico Interamericano, actualizado, sobre Privacidad y Protección de Datos Personales, el CONVENIO 108+ del CONSEJO DE EUROPA PARA LA PROTECCIÓN DE LAS PERSONAS CON RESPECTO AL TRATAMIENTO AUTOMATIZADO DE DATOS DE CARÁCTER PERSONAL; Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de carácter personal (1981) y su Protocolo Adicional (2001), aprobado por Argentina en 2019; todos los cuales han sido indefectiblemente considerados al momento de re pensar la normativa que debe velar por su protección.

En el presente acápite no se pretende realizar una nomenclatura reiteratoria de los instrumentos; no por carecer de valor jurídico, sino a los fines de posicionarnos mayormente en la importancia de su consideración local ceñida al comportamiento debido de la Administración frente a los datos a los que accede, máxime si se trata de automatización de información.

En efecto, los estándares se constituyen como reglas madre, como guías conductuales tácitamente aceptadas para arribar a una debida protección; de la que no escapa la Administración local, por cuanto reflejan la tendencia actual de la comunidad internacional. Las responsabilidades por el tratamiento indebido de los datos personales pueden y deben ser endilgadas también al sector público, razón por la cual las 'buenas prácticas' se presentan como un norte irrefutable, devenidas del fenómeno ya referenciado del *SoftLaw* internacional, como un derecho en constante formación con vocación de obligatoriedad y con basamento en la buena fe, con mas que habilita vínculos entre los gobiernos locales y el sistema internacional en un contexto de globalización y constante desarrollo.

Ciertamente, a decir de DEL TORO HUERTA los instrumentos de *derecho blando* internacional reflejan expectativas comunes de conducta cuya eficacia dependerá del grado de compromiso de cada Estado, que se presentan como una novedosa fuente de producción de derecho que ha ganado cada vez más espacio en la comunidad internacional, devenido asimismo del debilitamiento de los procesos de codificación y la proliferación de un nuevo orden global, con anclaje en el 'consenso generalizado' del debido proceder. En ese orden de ideas, el autor refiere que dichas normas sirven asimismo de 'inspiración' para los parlamentos en torno a la adopción de sus criterios en la legislación interna o para los jueces como pautas interpretativas reconociéndoles así, indirectamente, carácter obligatorio (de *HardLaw*).

Ello refleja que dicho fenómeno-del sistema internacional de derechos- es producto del mundo globalizado, siendo innegable su aceptación y uso en el derecho interno, al punto tal de ser basamento de numerosas legislaciones y decisiones judiciales y administrativas. Entonces, se presenta como un recurso fidedigno para reformas legislativas, incluso así se advierte en la expresión de motivos y fundamentos de los anteproyectos citados precedentemente.

El derecho supranacional ha irrumpido en el derecho público con el objeto de la adaptabilidad del ritmo de la realidad que nos circunda, en tanto hoy resultan impensadas las decisiones administrativas sin considerar los criterios de 'buen gobierno'. A decir de Daniel SARMIENTO, el *SoftLaw* 'unilateral' se presenta como la auto organización burocrática dentro de cada Administración, que habilita al Estado a ejercer potestades publicas mediante fórmulas atípicas de regulación, a saber: Circulares o Instrucciones que justamente direccionan formas de conducta internas dirigidas a los servidores públicos generando, así, compromisos de calidad en la prestación del servicio y potencian el derecho de los ciudadanos en relación con esa prestación.

Entonces, la acogida de las múltiples fuentes normativas -consideradas en todos sus aspectos- del derecho internacional del derecho público, impactan de manera directa en lo local impulsando no solo reformas legislativas, sino modos de hacer puertas adentro de la Administración, instaurando procesos internos de organización que prevengan conductas contrarias a los derechos protegidos de raigambre constitucional; entrelazando lo local, primigenio y originario con aquello de apariencia 'lejana' que se presenta como reglas de *Softlaw*.

En dicha inteligencia, no cabe duda alguna que lo que prima custodiar es la especial relación entre el sujeto -administrado- y la administración, vínculo que no puede escindirse de la temática que nos convoca; en la medida que actualmente esa relación se gesta -mayormente- en un contexto digital y de proliferación masiva de datos brindados por el particular al Estado; con basamento en la confianza y la buena fe en un pacto intrínseco; más careciendo de reglas claras en torno a su debido uso y tutela.

Esas reglas deben ser adoptadas del cumulo normativo obrante en el sistema de derecho público internacional y de los estándares de conducta que reclaman los organismos internacionales para los Estados nacionales y locales; por cuanto el norte es ciertamente guardar unicidad de criterios al momento de comportarse legítimamente ante la masividad del dato. Conforme ya se anticipara, la importación de procesos y procedimientos desde el derecho privado que impliquen un mejoramiento de la organización interna, hasta la creación desde el Estado local de reglamentos e instructivos de proceder frente al Big Data encuentran su basamento en los estándares internacionales, como guías de mínima y máxima para el 'buen hacer' en la gobernanza.

En otras palabras, no se reclama la creación de normas al efecto ni la invención de nuevos mecanismos de conducta; sino -en su caso- de la adopción de principios y reglas claras en torno a la tutela, uso y manipuleo de datos personales desde el Estado; lo que debe estar impregnado de aquellas buenas prácticas que emergen del consenso internacional.

Resulta palmario referenciar que el último Proyecto de Reforma de la Ley de Protección de Datos Personales (2023) se fundó justamente en actualizar la normativa imperante en pos de los mencionados estándares internacionales, marcando como fin último el derecho humano a la protección de datos personales y la autodeterminación informativa, la innovación tecnológica y la construcción de confianza a través de reglas de juego claras. El norte fue, y así lo establecen los fundamentos del Anteproyecto: armonizar la legislación argentina con los estándares internacionales y elevar las garantías de protección de la ciudadanía.

En dicha inteligencia, el Capítulo 5 del Proyecto hace mención a las obligaciones de los Responsables y Encargados del tratamiento de datos, instando la adopción de medidas para garantizar el cumplimiento de la norma y de políticas para el tratamiento de los datos personales. Del mismo se deriva, asimismo, el principio de responsabilidad proactiva del tratante de datos en tanto desarrollo de procesos internos para llevar a cabo de manera efectiva las medidas de responsabilidad y de procedimientos para facilitar a los titulares de datos la protección de sus derechos.

Ciertamente, dichas innovaciones legislativas -si bien, nuevamente, omiten referenciar al Estado como tenedor de datos y sujeto obligado, en tanto lo dispensan por sus funciones propias- fueron producto del consenso arribado previo numerosas mesas de dialogo con distintos actores del plano nacional e internacional en la materia[46], en tanto se convocaron audiencias y consultas públicas.

Sobre el particular y en el marco del documento arribado luego de las consultas realizadas -previo la redacción del Proyecto y citado *ut supra*-, estimo valioso mencionar que se mencionó en reiteradas oportunidades la necesidad de limitación a las excepciones al consentimiento como fuente de legitimidad, la incorporación de procedimientos y obligaciones ante vulneraciones de seguridad; como así también se remarcó la importancia

[46]https://www.argentina.gob.ar/sites/default/files/informe_consulta_publica_aaip.pdf

de establecer reglas claras para la cesión de datos entre organismos públicos y entre estos y empresas privadas.

En esta línea, se debatió sobre la necesidad de mejorar la interoperabilidad del Estado garantizando la protección de los datos personales; siempre armonizado con las normas internacionales; de reforzar los recursos en el Estado para poder afrontar los nuevos desafíos que presentan los cambios tecnológicos y se dio especial atención a la necesidad de establecer reglas claras y generar instancias de capacitación para los distintos agentes públicos, a fin de poder contar con instrumentos para velar por la protección de los datos personales. A su vez, se solicitó fortalecer las instancias de coordinación de la acción estatal de los distintos organismos públicos a fin de poder velar por los derechos fundamentales de la ciudadanía.

Todos los apuntes mencionados, que no fueron incorporados en forma directa en el Proyecto en tanto no se hace especial referencia al accionar del Estado frente a los datos, dan cuenta de la imperiosa necesidad de considerar la cuestión vinculada a la protección de datos personales desde la Administración Pública, tanto en su fas preventiva -capacitación al personal y desarrollo de reglas claras y procedimientos de resguardo-, como en su fas sancionatoria; determinando en debida forma los límites y alances de la excepción al consentimiento como fuente de legitimidad por las 'funciones propias' del Estado.

Se destaca que, en el Art. 17 inciso i) del Proyecto, que alude a la responsabilidad reforzada ante el tratamiento de datos sensibles, se referencia: "…*se prohíbe el tratamiento de datos sensibles, excepto si…i) Fuera necesario en ejercicio de las funciones y facultades de los Poderes del Estado en el cumplimiento estricto de sus competencias. Cuando los organismos públicos traten datos personales sensibles, deben proveer condiciones más estrictas de seguridad, lo que debe implementarse mediante salvaguardas apropiadas adicionales, diseñadas específicamente*…" Estimo propicio ello sea incorporado en la reglamentación de la ley, una vez sancionada, en tanto nuevamente la permisividad que se brinda al tratamiento de datos al Estado resulta sumamente amplia y genéricamente referenciada.

No debemos perder el foco, el escenario actual revela que cada vez más datos personales son recolectados, almacenados y utilizados, generando incluso nuevos datos a partir de ese tratamiento, todo lo cual el individuo que los proporciona desconoce

absolutamente; por lo que la protección de datos se ha convertido en una pieza fundamental, así como proporcionar un marco jurídico integral de conformidad a las pautas de regulación jurídicas establecidas en los Estándares de Protección de Datos en los Estados Iberoamericanos -modelo normativo flexible que responde a exigencias de nivel adecuado de protección- y un procedimiento interno que garantice su tutela efectiva.

La importancia, entonces, del control sobre el uso y tratamiento de datos personales desde el Estado radica no solo en cuanto a la privacidad, sino también a evitar prácticas ilegitimas tales como la vigilancia, analizar, predecir e incluso manipular el comportamiento de las personas, intercambio y difusión de datos entre los Estados y de inteligencia; todo lo cual asimismo reclama autoridades independientes para supervisar las prácticas del Estado. Frente a este nuevo escenario en el que predominan las tecnologías disruptivas, se torna particularmente necesario que los Estados adopten un marco normativo coherente y homogéneo, que debe prever el contralor asimismo de sus propias conductas.

CAPÍTULO III: EFECTOS DE UNA LIBRE E IRRESTRICTA CIRCULACIÓN DE DATOS SUMINISTRADOS POR PARTE DE LA CIUDADANÍA A LA ADMINISTRACIÓN PÚBLICA.

1.-El Administrado frente a la provisión de datos personales. Derecho Humano Fundamental a la intimidad y vida privada.

Ciertamente, resulta dificultoso parametrizar una perspectiva sin contar con un dato estadístico o empírico que refleje las específicas consideraciones de un grupo significativo de personas a las que aplica la situación de hecho, hoy generalizada mediante el acelerado avance e intromisión de Internet en la vida de los ciudadanos, claro está -y en lo que refiere a este trabajo- en su vinculación directa con el Estado.

Ahora bien, resulta indudable que el ciudadano se encuentra enmarcado en un sistema que le exige determinados comportamientos direccionados a obrar dentro de los mecanismos

que lo habiliten a la provisión de servicios y al ya referido vínculo con la Administración local.

En efecto, el 'comportamiento' de los Administrados -en la mayoría de los casos- siquiera es producto de una decisión razonada y optada, sino mas bien un obrar automatizado, exigido por el Estado; en el que la provisión de datos se presenta como una mecánica autorizada y admitida tácitamente, sin cuestionamientos.

Sobre el particular, no puede dejar de pensarse de qué manera esa intromisión deliberada y 'consensuada' choca directamente con el derecho a la intimidad y la vida privada de los ciudadanos, cuestionando cual es el real y certero limite que debe considerar el Estado para actuar dentro de los parámetros legales y habilitados.

Ello así, surge una innegable comparación con las limitaciones que se evidencian –en el ámbito de las relaciones entre particulares- cuando de circulación de datos se trata; una tutela que se presentaba -hace no mucho tiempo- posterior a la circulación del dato y, actualmente, con la naciente presencia de un mercado único digital y proyección de una Administración netamente digital, con consideraciones preventivas, de consentimientos anticipatorios y de una marcada cultura de la privacidad que conforma el patrimonio moral de las personas, presentando un anhelado nivel de protección en una clara evolución a nivel jurídico normativo en lo que refiere al reconocimiento de derechos, con una notable injerencia del derecho internacional.

Ciertamente, el derecho a la autodeterminación informativa reconoce el derecho al honor, a la intimidad personal y familiar e incluso a la propia imagen del individuo; todos derechos personalísimos y vinculados a la dignidad humana y al resguardo de su información, convirtiendo el garantismo en parte fundamental del ejercicio del derecho y del propio Estado.

Al respecto, el derecho a la intimidad es un elemento esencial de la libertad personal constituido por el derecho a la protección de datos, que corresponde a una parte de la ejecución plena de las libertades otorgadas. Al elevarse el derecho a la vida privada al rango de derecho 'fundamental', habilita la tutela para impedir la intromisión no autorizada de funcionarios públicos o de otros individuos respecto a aspectos de datos personales otorgando, de esta manera, mayor seguridad a los ciudadanos, reafirmando el principio de

seguridad jurídica, desagregando no solo la confianza en la administración de justicia sino también en las normas emitidas por los legisladores.

El tratadista Germán Bidart Campos se refiere a la intimidad y a la privacidad, de la siguiente manera: "la intimidad es la esfera personal que está exenta del conocimiento generalizado de tercero... y la privacidad es la posibilidad irrestricta de realizar acciones privadas (que no dañen a otros) que se cumplan a la vista de los demás y que sean conocidas por estos"[47].Evidenciada la diferencia entre la intimidad y la privacidad, se puede colegir que estos son dos conceptos que, analizados bajo criterios únicamente de semántica, se podrían entender como sinónimos, cuya trascendencia a nivel universal genera una asimilación del derecho en demanda de su protección, ocasionando que su vulneración involucre una clara intromisión personal.

En lo que respecta a la protección de los mismos, se debe tomar en cuenta que la intimidad al ser considerada como un bien jurídico protegido, y más aún un derecho fundamental, mantiene una gama de protección singularizada y complementaria con la privacidad.

Por su parte, la privacidad presenta un alcance que se entiende compatible con la intimidad, sin llegar a la premisa de que son diferentes, hasta el punto de generar como conclusión un silogismo de premisas mayores y menores: "los asuntos íntimos son privados, pero no todos los asuntos privados pueden tener carácter de íntimos". Es decir, cuando se vulnera la intimidad, que engloba áreas muy concretas de la vida de una persona, se ha vulnerado a la vez a la privacidad o aspectos generales referentes a una persona; pero cuando se ha vulnerado la privacidad, no necesariamente significa que se ha atentado contra la intimidad sin perjuicio de que efectivamente pueda llegar a producirse.

Entonces, la intimidad como derecho fundamental protege la esfera más privada de los individuos, dotada de caracteres reservados que pueden o no compartirse con autorización, y se encuentra tutelado constitucionalmente. Sin embargo, es esencial recordar que este derecho, como tal, no es absoluto –lo mismo sucede con la protección de datos-, estas son prerrogativas que deben ejercerse dentro de límites razonablemente impuestos,

[47]Germán Bidart y Walter Carnota, *Derecho constitucional comparado* (Buenos Aires: Ediar, 1998), 137.

condicionado a ciertas circunstancias que justifiquen la posibilidad de vulnerarlo en diversas expresiones de 'necesidad o interés público'.

Sin embargo, la afirmación de ese interés público para justificar el sacrificio del derecho a la intimidad, y por lo tanto a la entrega de datos, no es suficiente para que la garantía constitucional de este pierda concreción; por lo tanto, no es solo la regularidad formal de la decisión que motive el hecho de acuerdo al marco jurídico normativo vigente, sino también la sana crítica y razonamiento de la autoridad actuante, ya sea en el ámbito judicial o administrativo claramente vinculados al revestimiento de la atribución de limitar el derecho a la intimidad.

Por lo tanto, debe presentarse una necesidad absoluta respecto de la toma de esa decisión, considerando la concurrencia de una situación específica que genere de forma intrínseca la justificación de la limitación de derechos y principalmente de establecer la estimación de proporcionalidad de los bienes jurídicos y la situación en que se halla aquel individuo a quien se la impone.

Habrá entonces que ponderar siempre el interés público para justificar el sacrificio del derecho a la intimidad. Lo trascendental en este punto es corroborar si el administrador logrará alcanzar una justificación constitucional objetiva y razonable de las cuestiones que le han llevado a ejecutar esta medida de intromisión de la intimidad.

Dicho lo anterior es necesario, para la Administración, considerar la transferencia de datos como causa ineludible de la titularidad del derecho a la intimidad y el innato poder de control de datos, con el fin de determinar con facilidad la posible vulneración de derechos personales en la actual evolución tecnológica, vinculando el análisis a la expresión de la voluntad del titular con la existencia de la autorización.

El avance de la sociedad conjuntamente con el desarrollo tecnológico va generando la aparición de nuevos riesgos a la intimidad, en el que el propietario o titular del derecho confiere o transfiere el poder y control de su información y/o de sus datos, plasmándolo quizá en la premisa exagerada de dotar a otro el poder de uno mismo y de su propia información. Esta transferencia -de nuevo, casi automatizada- genera una visión de protección alterada y hasta de carácter indirecto de un derecho constituido como innato y fundamental.

En este sentido, el análisis jurídico correcto para determinar la violación del derecho a la intimidad a nivel general, tanto dentro del ámbito público como privado, subyace en la determinación de aquella ausencia de un consentimiento válido para acceder a la información o del consentimiento para utilizarla de manera específica, en tanto y en cuanto la acción relevante será la forma de obtención de dicha información, debiendo determinar si esta fue entregada de forma legítima (autorización) y sin embargo fue utilizada para un fin distinto para el que fue otorgada, o no; o si simplemente la ausencia de la respectiva autorización es latente, partiendo de esta base podemos enfocarnos en la existencia de la posible lesión del derecho a la intimidad.

He aquí donde cobran relevancia los principios plasmados en la normativa internacional referidos a la protección de datos por parte de los Estados, al correcto y uso y manipuleo de los mismos, y a la toma de conciencia del acervo al que acceden mediante la masividad del *big data* conferido por los ciudadanos.

Resulta necesario abordar el papel del Estado en la tutela de derechos y su capacidad de injerencia en la intimidad de sus ciudadanos y, para ello, deviene indispensable referirse a la Sentencia de la Corte Interamericana de Derechos Humanos del Caso Artavia Murillo y otros *vs.* Costa Rica, sobre la "fecundación in vitro" del 28 de noviembre de 2012[48], caso en el cual se puede evidenciar el exceso de poder en el uso de las prerrogativas exorbitantes del Estado y el alto nivel de intromisión y vulneración al legalizar la prohibición de métodos artificiales de concepción (fecundación in vitro), generando circunstancias inconcebibles que se pueden producir por el hecho de no reconocer derechos naturales, fundamentales e innatos, amparados en justificaciones no proporcionales respecto del bien jurídico a proteger y el bien jurídico finalmente perjudicado.

Es evidente la intervención invasiva del derecho a la autodeterminación individual que recae sobre la libre elección de procreación, ya sea mediante el uso de medidas directas o bajo el uso de mecanismos artificiales, vulneración que engloba la autonomía personal y libertad de llegar a ser progenitor y todas aquellas decisiones que engloban la esfera más íntima de la vida privada y familiar del ser humano y que forman parte del ejercicio de las libertades personales universalmente reconocidas.

[48]https://www.corteidh.or.cr/docs/casos/articulos/seriec_257_esp.pdf

En este caso, la dignidad humana fue objeto de constantes violaciones, incluso a nivel mediático, ya que se divulgó variada publicidad de carácter discriminatorio y estigmatizante en contra de la situación de desventaja de los accionantes, evidenciando su estado de incapacidad de concebir, y emitiendo juicios de valor respecto de la infertilidad, provocando daños en los derechos personales y en el patrimonio moral de los accionantes a causa del linchamiento mediático constituido.

La violación referida se evidencia en la clara exposición de información privada en los medios de comunicación, en ausencia del elemento que prevendría la configuración de un delito, y se constituye como la expresión volitiva que demuestre un consentimiento expreso de la divulgación de información (autorización), generando daños morales.

Dicho lo anterior, es necesario mantener un análisis respecto de la información consolidada a nivel público, ya sea dentro de bases datos, ficheros y/o información generada o incluida en sistemas electrónicos. Cabe recalcar que como ciudadanos y en ejercicio de nuestro estatus generamos información pública y privada que se va consolidando en las diferentes instituciones del mismo carácter.

Ahora bien, esas bases de datos generan asimismo un sistema de interconexión de 'control cruzado' de la información de los ciudadanos, razón por la cual nace la duda de ¿hasta qué punto es procedente y positivo un enlace y conexión de toda la información ciudadana? Considerando que ello supone la concurrencia de dos elementos esenciales: el primero es la existencia de un determinado estándar normativo de conocimiento tanto del agente controlador, como del individuo que es objeto de dicho control o actividad; y el segundo es la formulación por la "autoridad" o "agente de control" de un juicio o premisa adecuado respecto del carácter informativo a vincular, con el objeto de salvaguardar la seguridad jurídica correspondiente en la conexión de datos, previniendo que las actuaciones administrativas no excedan de sus facultades.

Una vez que el titular transfiere la información al Estado y este la obtiene se configura un vínculo entre ambos, en el cual el Estado tiene que garantizar su protección mediante el principio de seguridad y principio de confidencialidad de los datos, resguardando la referida información de manera que no pueda existir ningún riesgo de divulgación. Es indispensable recalcar que el requisito imprescindible para delimitar si estos derechos han sido o pudieron haber sido violados, se lo consigue bajo el análisis de los actos presuntamente lesivos, y si

estos se efectuaron con o sin la correspondiente autorización del sujeto, es decir, con el respectivo consentimiento que cabe mencionar puede ser revocado en cualquier momento.

En este sentido, lo óptimo a nivel legislativo sería que se establezca taxativamente en qué casos no se apreciará la existencia de intromisión ilegítima en el ámbito protegido como en el caso de que estuviere expresamente autorizada por ley, o, en su defecto, cuando el titular del derecho hubiere otorgado al efecto su consentimiento expreso.

En este punto, la Constitución no solo tiene como objeto la protección de la vida de la persona frente a cualquier tipo de invasión, tomando en cuenta que el individuo desea excluir del conocimiento público y de las intromisiones de terceros, información que un sujeto la determina como suya y personal, por lo tanto es el derecho a la protección de datos el que tiene como objeto garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho afectado.

De lo anterior, el derecho a la intimidad le permite al individuo excluir cierta información del conocimiento público, y resguardar sus datos personales de una publicidad no voluntaria, y el derecho a la protección de datos reconoce al individuo la facultad de controlar sus datos personales y a su vez la capacidad de disponer y decidir sobre los mismos. Tal es así que el derecho a la protección de datos garantiza al ciudadano la forma de uso de estos, es decir, el individuo tiene poder de disposición sobre los mismos, a esta facultad hay que agregarle la posible dificultad del ejercicio de este poder con el hecho de desconocer qué datos se encuentran en posesión de terceros, quienes los poseen y con qué finalidad, máxime cuando ese tercero es el Estado.

En este sentido, el llamado derecho a la protección de datos lleva consigo arraigado un contexto evolucionado, tomando en cuenta que este extiende las garantías del derecho a la intimidad en su dimensión constitucionalmente protegida, y abarca los bienes de la personalidad que se refieren a la vida privada vinculada a cualquier tipo de dato personal en el uso de las nuevas tecnologías, conteniendo en su haber la autodeterminación informativa conceptualizada como aquella necesidad de que los ciudadanos controlen la información que les concierne, ya no como un mero derecho de defensa frente a las intromisiones de otros, sino ahora, y frente a los riesgos tecnológicos, como un derecho activo de control sobre el flujo de informaciones que circulan sobre nosotros.

La autodeterminación informativa comporta el derecho de toda persona a ejercer control sobre la información personal que le concierne, frente a cualquier ente público o privado, como ya se anticipara *ut supra*. Cabe mencionar que este derecho fue utilizado por primera vez por el Tribunal Constitucional Federal de Alemania, en la sentencia sobre la Ley del Censo del 15 de diciembre de 1983, con la que se faculta a las personas a decidir y consentir de manera informada y libre el uso de sus datos personales por terceros, ante el tratamiento automatizado de los mismos.

Es así que el derecho a la protección de datos personales se deriva del derecho a la vida privada y por lo tanto del derecho a la intimidad, los cuales no dejan de verse amenazados por las nuevas tecnologías que modifican formas de distribución de la información y hasta de almacenamiento.

Sin embargo, proyectando el uso tecnológico para plasmarlo en el derecho positivo para llegar al bien común, se debe mencionar la necesidad de promulgación de leyes y políticas públicas que establezcan límites a la libertad humana y que generen un equilibrio entre los derechos propios y ajenos, como principios básicos de toda sociedad, aplicables asimismo al uso y tratamiento que de los mismos haga el Estado.

Todo lo antedicho no hace más que reflejar la imperiosa necesidad de sistematizar un mecanismo afín, puertas adentro de la Administración Pública local que logre, por un lado, controlar el debido uso y tratamiento de los datos conferidos por la ciudadanía y, por otro, disminuir los posibles efectos colaterales que podría conllevar una intromisión inadecuada en la vida privada de las personas, a través de una utilización incorrecta de la información provista; en tanto el alcance de un manipuleo irrestricto de datos atraviesa y conculca en forma directa derechos humanos fundamentales de los individuos.

CONCLUSIONES: DESAFIOS EN LA ERA DIGITAL

A los fines de representar lo analizado en el presente trabajo, considero pertinente desarrollar el presente capitulo -de particular relevancia- en una metodológica división que permita reflejar el contenido de lo estudiado desde las ópticas planteadas en los objetivos.

Consecuentemente, he optado por dividir las conclusiones bajo los siguientes subtítulos y como 'dinámicas' (entendidas como las interacciones de los procesos en pos de un objetivo común); sin que ello implique escindir las temáticas, sino meramente a los fines ordenatorios y para mayor claridad al lector, a saber: 1) Dinámica organizacional respecto al acceso, uso y manipuleo de datos personales por parte de la Administración Pública Local; 2) Dinámica de la normativa internacional en torno a la protección de datos personales frente a la Administración Pública local y global; 3) Dinámica del Administrado frente a la provisión de datos personales.

1) <u>Dinámica organizacional respecto al acceso, uso y manipuleo de datos personales por parte de la Administración Pública Local</u>.

En lo que respecta la Administración Pública local, los límites frente al debido uso, manipuleo y gestión de datos personales se presentan como difusos e insuficientes, en tanto no solo no existe adecuación a la normativa nacional -amen de su innecesaridad por la derivación lógica de protección de derechos constitucionales-; sino tampoco efectiva y positivada subsunción a los principios y normas internacionales -que conforman el *SoftLaw* internacional- que rigen la materia.

Ello refleja que, a nivel local, no existe un mandato de control de oficio sobre la cuestión, menos aún un organismo concreto dotado de las competencias para tal fin. En efecto, el control es posterior, desde el individuo y cuando el daño ya se ha concretizado.

En otras palabras, no existe un sistema organizacional y procedimental reglado -puertas adentro del Estado Provincial- que regule de qué manera deben recabarse y protegerse los datos personales a los que se accede, con mas que el manejo de los datos personales es muy diferente en el ámbito público que el privado, como responsabilidad adicional en materia de transparencia y tutela.

Asimismo, se evidencian dos alternativas posibles: desconocimiento en la materia, en tanto tampoco se verifican propuestas de capacitaciones intra Administración; o decisión discrecional en torno a omitir el tratamiento de la cuestión, cobrando relevancia el concepto 'interés público' para un manipuleo discrecional de los datos, por lo que quedara en el arbitrio de y buen juicio del sujeto obligado la interpretación de los conceptos, y será solo a

través de una sólida concientización y capacitación especializada, que se lograra que la autoridad no abuse de los espacios de apreciación subjetiva, para imponer límites a la protección de datos.

En ese contexto, se pone de resalto la digitalización de la vida social y en relación (sobre todo el vínculo Estado-Sociedad), maximizada en los últimos años; por lo que emerge como mandatorio repensar y plantear un efectivo mecanismo de control de los datos personales, con el norte en un tratamiento licito, leal y transparente, con basamento en los principios emergentes de los comportamientos en el ámbito internacional -sobre todo en los conceptos de 'consentimiento previo' y el naciente derecho a la autodeterminación informativa'- y con obligada tutela de los derechos constitucionalmente consagrados.

A ello debe añadirse la debida capacitación de los agentes en la materia, con el objeto de generar un arraigado concepto de responsabilidad social de las administraciones públicas y 'rendición de cuentas' ante la sociedad, mediante la publicidad de la información y el mayor acceso a los datos públicos -brindando transparencia a los procesos- y participación ciudadana, en un claro recupero de confianza y con basamento en el principio de colaboración del individuo hacia el Estado (ruptura del concepto de "obediencia").

Esto haría a un indudable bloque de protección preventiva y accesibilidad, conformado por la protección preventiva del dato y el acceso a la información pública, enfatizando la necesidad de protección de la vida privada de las personas, con el objeto de evitar que la entrega masiva de datos sin control se transforme en una fuga de información personal sin restricciones.

La propuesta se presenta como un esquema organizacional transversal y competencialmente concurrente, que contemple la creación de organismos de control y fiscalización eficientes, competentes y, sobre todo, independientes, que propendan a un efectivo y adecuado tratamiento de los datos personales por parte del Estado, con reglamentación de pautas y reglas basadas en los principios internacionales estandarizados de finalidad, adecuación, pertinencia de datos y responsabilidad proactiva, propendiendo a un análisis de riesgo para evitar fugas masivas en los sistemas estatales.

2) Dinámica de la normativa internacional en torno a la protección de datos personales frente a la Administración Pública local y global.

El sistema de derecho administrativo global, conformado por principios internacionales caracterizados por el *SoftLaw*, no solo habilita la implementación de mecanismos internos amparados en diversas fuentes de derecho por fuera de las normas tradicionales, sino también interpela a considerar el mundo del derecho en general, con el norte en los derechos humanos fundamentales.

En esa dinámica, y siendo la persona el eje central, el ordenamiento jurídico local debe pensarse desde la óptica de las reglas y conductas internacionales, para garantizar la sistematización de los procedimientos de la manera que mayor se amalgamen con el respeto debido al ser humano, en pos de su pertenencia al plano internacional, y siendo el eje de toda decisión razonablemente pensada.

Dichos preceptos cobran hoy mayor relevancia, al estar transitando la era de la sociedad de la información, del desarrollo de un mercado digital y un Estado cada vez más globalizado (con la proliferación masiva de datos); que obliga a repensar el vínculo Estado-sociedad desde la perspectiva de la participación activa del ciudadanos en los temas que a él le conciernen y con carácter preventivo siendo, el consentimiento previo, el punto álgido y significativo de inflexión para el debido ejercicio del derecho de autodeterminación informativa.

Se reitera, entonces, que el sistema -conformado por reglas, estándares y principios- ya existe (como reglas de mínima y de máxima), siendo función de la Administración local adaptarlo puertas adentro del Estado, de manera transversal y como parte integrante de la nueva gobernanza con reglas claras.

Frente a este nuevo escenario, en el que predominan las tecnologías disruptivas, se torna particularmente necesario que los Estados adopten un marco normativo coherente y homogéneo, que debe prever a enaltecer el contralor de sus propias conductas.

3) Dinámica del Administrado frente a la provisión de datos personales.

En lo que respecta a los Administrados, la nueva era digital exige un comportamiento activo de los ciudadanos frente al Estado, máxime en lo que respecta a la provisión de datos personales, esto es conocer los alcances y limitaciones de dicha provisión, en tanto no pueden estudiarse los datos personales sin asociarlos a un individuo sujeto de derechos y obligaciones.

En dicho especial vínculo cobra preponderante relevancia la tutela del derecho a la intimidad y vida privada de los individuos, de carácter preventivo, de consentimiento anticipado y de una marcada cultura de la privacidad que conforma el patrimonio moral de las personas, máxime en lo que respecta a la transferencia de datos dentro de la Administración.

En ese contexto, el derecho a la autodeterminación informativa reconoce el derecho al honor, a la intimidad personal y familiar e incluso a la propia imagen del individuo; todos derechos personalísimos y vinculados a la dignidad humana y al resguardo de su información, convirtiendo el garantismo en parte fundamental del ejercicio del derecho y del propio Estado.

Ello así, asimismo, se reclama un marco jurídico que reglamente los parámetros de 'interés público' como habilitante del tratamiento del dato, con más la sana crítica y el principio de la razonabilidad implementado en las decisiones de la autoridad, que justifiquen la limitación de los derechos referenciados.

Lo antedicho no hace más que reforzar la necesidad de reglamentar un procedimiento que determine el ámbito de protección, la necesidad de consentimiento previo a la accesibilidad de los datos y las limitaciones de su circulación y uso, para evitar una intromisión inadecuada en la vida de las personas.

RFFLEXIONES FINALES:

Deviene innegable que la casuística aún no ha atravesado un margen temporal de apreciación que permita extraer conclusiones adecuadas acerca del mecanismo más certero para tutelar los datos personales que ingresan a la Administración Pública, como fenómeno social propio de la era digital; siendo que asistimos no solo a un derecho en formación (autodeterminación informativa), sino a mecanismos y procedimientos nacientes en forma

concomitante con la sociedad digital, en constante y dinámico cambio, todo lo cual deja de manifiesto la vulnerabilidad de los datos personales cuando estos viajan por medios electrónicos, físicos o plataformas estatales.

Ahora bien, tomando las propuestas derivadas de la reglamentación local del acceso a la información pública y el expediente digital, con más los lineamientos esbozados en la Comisión de Trabajo sobre Gobernanza de Datos y protección de la privacidad del Consejo Federal para la Transparencia, toda parámetros rectores que conforman –a mi entender- el norte de la nueva gobernanza en lo que respecta a una Administración digitalizada, con basamento en el *Soft Law* internacional; no puede obviarse que la vía correcta sería sistematizar y reglamentar un mecanismo de control preventivo, que determine las vías adecuadas para el acceso a un consentimiento expreso y previo (el que podría ser asimismo digital, es decir sin requerir la comparecencia personal) -como recaudo elemental para un uso licito de la información 'desagregada' que pueda extraerse-, con más la necesaria positivización de los conceptos relevantes en la materia en correlato a lo local (vgr. 'interés público', 'dato personal y sensible', entre otros) y las consecuentes capacitaciones en la temática para todo agente que se desempeñe en la Administración local, y para la ciudadanía.

En este último punto, se demandara un conocimiento y aprendizaje en la materia especifico a fin que los sujetos obligados cumplan con sus obligaciones, además de afrontar un desarrollo tecnológico vertiginoso y su colateral creciente almacenamiento de información, lo que exige respuestas institucionales programáticas y adecuadas, para el cumplimiento de la obligación estatal de proteger los datos personales de las personas.

Esta obligación estatal emerge como una manda inherente de la función propia del Estado y sus organismos, lo que maximiza el deber legal y moral de cumplir la ley y reflejar, ante la sociedad, el debido tratamiento y resguardo de los datos personales, en un rol de conducta ejemplar, con el enfoque en el ser humano como ser social y en relación.

Sobre el particular, la creación de un órgano de control independiente permitiría una correcta aplicación de la reglamentación a crearse la que, indudablemente, atravesara en forma transversal toda la Administración, por cuanto los datos ingresan a través de un sinnúmero de mecanismos; a saber: gestión de expedientes, solicitud de turnos, presentaciones de peticiones y reclamos, otorgamiento de becas y subsidios, altas en

sistemas internos, utilización de Apps gubernamentales, entre otros, todo lo cual maximizará la percepción de la ciudadanía acerca de la efectiva tutela de sus datos personales.

A ello debe añadirse que asistimos, sin lugar a duda, a la creación de un bloque constitucional legal que compone y compondrá la temática de datos e información digital, todo lo cual no puede escindirse y tratarse como compartimientos estancos, conformando el basamento para un Estado confiable y accesible, nuevamente, en un vínculo Estado-Sociedad que posicione al individuo como sujeto central de derecho y prioritariamente considerado, siempre teniendo en miras la incorporación de aquellos sujetos que han quedado por fuera de la digitalización.

Lo referenciado en el párrafo precedente, y a modo de conclusión final, no puede escindirse del fenómeno del correcto empleo de los grandes volúmenes de datos y los significativos resultados que podría implicar el análisis del Big Data, a los fines de tratar la información desde diversos sectores para la gestión de gobierno, incorporando a las soluciones transaccionales de la gestión digital de sus procesos dicho acervo, lo que les permitirá evolucionar y avanzar en sus capacidades de gestión y análisis de la información que poseen, gestionan e intercambian con otros organismos y, consecuentemente, mejorar el servicio que se brinda al ciudadano.

Esto es la llamada 'estrategia de datos abiertos' (cuanto mayor es el grado de apertura de datos, mayor es el tamaño y la diversidad de la comunidad que accede a ello), logrando una participación de verdadero valor del ciudadano, por cuanto no debemos olvidar que la información es producida por la sociedad y las prácticas de análisis del Big Data deben estar integradas con los principios del tratamientos de datos personales siendo el hombre, como ser social, el principal motivo de logar una retroalimentación mutua y que propicie el justo intercambio, minimizando el riesgo que este análisis masivo crea sobre la privacidad y datos personales.

En suma, se demanda una responsabilidad proactiva, aumentada, eficiente y conocedora con respecto al tratamiento de datos personales, en un ético manejo de la información, aplicando una Plan, Guía, Lineamientos, Procedimientos y reglamentación acorde a la nueva era digital, que genere confianza en el ciudadano de a pie en torno a un debido uso de la información. No se trata solo de un deber genérico de protección, sino de un plan de acción basado en los estándares desarrollados

VI. BIBLIOGRAFÍA:

1) Convención Americana sobre Derechos Humanos (Pacto de San José de Costa Rica). O.E.A. (1969) https://www.oas.org/dil/esp/tratados_b32_convencion_americana_sobre_derechos_humanos.htm.
2) COMUNICACIÓN DE LA COMISIÓN AL CONSEJO, AL PARLAMENTO EUROPEO, AL COMITÉ ECONÓMICO Y SOCIAL EUROPEO Y AL COMITÉ DE LAS REGIONES. "El papel de la administración electrónica en el futuro de Europa". Bruselas, 26.9.2003. http://www.hfernandezdelpech.com.ar/PDF-%20comisionComuniEuropeas-ProtecDatosPers.pdf.
3) Reglamento (UE) N° 2016/679 del Parlamento Europeo y del Consejo 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). 27.04.2016.https://www.ugr.es/sites/default/files/2017-08/CELEX_32016R0679_ES_TXT.pdf
4) Estándares de Protección de Datos Personales para los Estados Iberoamericanos. Red Iberoamericana de Protección de Datos. 20.6.2017. https://www.redipd.org/sites/default/files/inlinefiles/Estandares_Esp_Con_logo_RIPD.pf
5) Informe N° 638/21 del Comité Jurídico Interamericano. Principios actualizados sobre Privacidad y Protección de Datos Personales. O.E.A. 2021. http://www.oas.org/es/sla/cji/docs/CJI-doc_638-21.pdf
6) BASTERRA, MARCELA. "El consentimiento del afectado en el proceso de tratamiento de datos personales". Jurisprudencia Argentina. Número Especial, 28 de abril de 2004, pág. 6 http://marcelabasterra.com.ar/wp-content/uploads/2016/11/HD.-El-consentimiento-del-afectado-en-el-proceso-de-tratamiento-de-datos-personales.pdf
7) KINGSBURY, KRISCH, NICO KRISCH Y STEWART, RICHARD B. "El surgimiento del Derecho Administrativo Global", sin fecha
8) Res. N° 01/2020 CIDH.https://www.oas.org/es/cidh/decisiones/pdf/Resolucion-1-20-es.pdf
9) Objetivos de Desarrollo Sostenible 2030 Provincia de Entre Ríos: https://www.entrerios.gov.ar/modernizacion/index.php?codigo=113&modulo=
10) BROUN ISAAC, JORGE TOMAS. "Desafíos constitucionales en torno a la tutela del derecho de acceso a la información y libertad de expresión en la era digital". ANUARIO DE DERECHO CONSTITUCIONAL LATINOAMERICANO. AÑO XXVI, BOGOTÁ, 2020, PP. 749-771, ISSN 2346-0849.

11) ABRAMOVICH, VÍCTOR. "De las violaciones masivas a los patrones estructurales: nuevos enfoques y clásicas tensiones en el sistema interamericano de derechos humanos", sin fecha.
12) GRIFFERO, ANDRÉS. "El derecho de acceso a la información pública en argentina y el derecho de protección de datos personales. a propósito de la ley nº 27275". R.I.T.I. nº 4 Mayo-Agosto 2017.http://revistainternacionaltransparencia.org/wp-content/uploads/2017/08/6.-Andr%C3%A9s-Griffero.pdf
13) TOSTADO, MARÍA DEL CARMEN, MONTEVERDE VALENZUELA, MARÍA DE LOS ÁNGELES, OCHOA MEDINA, IVON EDITH. "La transparencia como estrategia para el cumplimiento del objetivo de desarrollo sostenible 16 de la agenda 2030: paz, justicia e instituciones sólidas", sin fecha. http://www.memoriasconvision.uson.mx/memorias/2020/MemoriasConvision2020.pdf#page=184
14) MONLEON GETINO, ANTONIO. "El impacto del Big-data en la Sociedad de la Información. Significado y utilidad". Universidad de Barcelona. (2015).
15) VECINDAR, LAURA. "Sistemas de información y prácticas de vigilancia en la protección social: controversias, tensiones y desafíos para el Trabajo Social" Rev. Plaza Pública, Año 13 - Nº 23, Jul. 2020. ISSN 1852-2459.
16) NOGUERA OSORIO, MACARENA. "Nuevo marco regulatorio de la protección de datos personales y protección de la vida privada en Chile". artículo académico presentado a la facultad de derecho de la Universidad Finis Terrae, para optar al grado de magister en derecho público: transparencia, regulaciones y control. Santiago, Chile. 2020. http://repositorio.uft.cl/bitstream/handle/20.500.12254/1892/Noguera_2020.pdf?sequence=1&isAllowed=y
17) QUINTANILLA MENDOZA, GABRIELA. "Legislación, riesgos y retos de los sistemas biométricos". Universidad Pedagógica Nacional. México. Rev. chil. derecho tecnol. vol.9 no.1 Santiago jun. (2020). http://dx.doi.org/10.5354/0719-2584.2020.53965
18) NOUGRERES, ANA BRIAN. "El sistema legal uruguayo de protección de datos personales". Universidad de los Andes. Facultad de Derecho. Revista de Derecho, Comunicaciones y Nuevas Tecnologías. 2007.https://dialnet.unirioja.es/servlet/articulo?codigo=7510287
19) GUZMAN GARCÍA, MARÍA DE LOS ÁNGELES. "El derecho fundamental a la protección de datos personales en México: análisis desde la influencia del ordenamiento jurídico español". universidad complutense de Madrid. facultad de derecho. Madrid, 2013.
20) FRESCURA TOLOZA, DIEGO EMILIO. "Debates públicos en torno a la creación del Sistema Federal de Identificación Biométrica (SIBIOS): tensiones entre seguridad y privacidad". XIII Jornadas de Sociología. Facultad de Ciencias Sociales, Universidad de Buenos Aires, Buenos Aires, 2019.

21) ARROYO JIMENEZ, LUIS. "Ponderación, proporcionalidad y Derecho administrativo". Revista para el análisis del derecho. Madrid, 2009.
22) REYNA, JUSTO J. "Globalización, pluralidad sistémica y derecho administrativo: apuntes para un derecho administrativo multidimensional". Revista de Derecho Administrativo y Constitucional. Ed. Forum. Belo Horizonte, 2011.
23) REYNA, JUSTO J. "La reforma de la Administración Pública local para la tutela de los derechos fundamentales en el siglo XXI". Pgs. 35-82. Revista de Derecho Administrativo y Constitucional. Ed. Forum. Belo Horizonte, 2014.
24) FELER, ALAN M, "SoftLaw como herramienta de adecuación del derecho internacional a las nuevas coyunturas", pp. 281-303. Lecciones y Ensayos nro. 95. 2015.
25) LAZCOZ MORATINO, G y CASTILLO PARRILLA, JOSE A, "Valoración algorítmica ante los derechos humanos y el Reglamento General de Protección de Datos: el caso SyRI", Rev. chil. derecho tecnol. vol.9 no.1, Santiago jun. 2020. http://dx.doi.org/10.5354/0719-2584.2020.56843
26) REZZOAGLI, LUCIANO. "Guía para estudios universitarios y de posgrado" Universidad Autónoma de Durango. Ed. Fomento Educativo y Cultural Francisco de Ibarra A.C. México, 2009.
27) VILLAR PALASI, JOSE LUIS y VILLAR ESCURRA, JOSE LUIS. "El ordenamiento jurídico argentino". Lección 1.
28) VILLAR PALASI, JOSE LUIS y VILLAR ESCURRA, JOSE LUIS. "Principios del derecho administrativo" TOMI I. "Concepto y fuentes". Madrid, 1987.
29) ALEXY, ROBERT. "Sistema jurídico, principios jurídicos y razón práctica". DOXA (5), 1988.
30) MAGALDI, NURIA. "El concepto de procura existencial en Ernst Forsthoff y las transformaciones de la administración pública". Revista de Derecho Público: Teoría y Método. Madrid, 2020.
31) FIORINI, BARTOLOME. "El estado y los procesos estatales". Capitulo Segundo.
32) BALBIN, CARLOS. "Manual de Derecho Administrativo". Cap. 5 "Las fuentes del derecho administrativo". Segunda Edición, Ed. La Ley.
33) UTRILLA FERNANDEZ- BERMEJO, DOLORES. "La relación jurídica en el sistema de derecho administrativo". Revista de derecho Público: Teoría y método. Madrid, 2020.
34) MARIENHOFF, MIGUEL S. "TRATADO DE DERECHO ADMINISTRATIVO. Administración Pública. Derecho administrativo. Estado y Administración Pública. Organización administrativa". Tomo I.
35) NAVAS QUINTERO, ANDRES. "La nueva gestión pública. Una herramienta para el cambio". Revista Mundo. Colombia. 2010
36) PICCIRILLI, MARIA EUGENIA. "Principios Nacionales e Internacionales en el marco de la Protección de Datos Personales. Deficiencias. Recomendaciones" SID 2015, 15º Simposio Argentino de Informática y Derecho.

37) Asociación por los Derechos Civiles (ADC). “El Estado recolector. Un estudio sobre la Argentina y los datos personales de los ciudadanos”.http://www.adc.org.ar/wp-content/uploads/2014/09/El-estadorecolectorInformeADC.pdf. (2014)
38) BALBIN, CARLOS F. Crisis del derecho administrativo. Bases para una nueva teoría general. Ed. Astrea. 2020.
39) CANYELLES, JOSEP MARIA. Responsabilidad social de las administraciones públicas. Revista de Contabilidad y Dirección. Vol. 13, año 2011, Págs. 77-104.
40) GAETE QUEZADA, RICARDO ANDRÉS. “Aplicaciones de la responsabilidad social a la nueva gestión pública”. Universidad de Antofagasta, Chile. 2008.
41) DOHMANN, INDRA. “Derecho Administrativo e incertidumbre”.
42) BARNES, JAVIER. “La transposición de valores públicos a los agentes privados por medios de organización y procedimiento”.
43) DRUCAROFF AGUIAR, ALEJANDRO. “Ética pública, funcionarios y conflictos de intereses. Publicado en: LA LEY 21/07/2016, 21/07/2016, 1. Cita Online: AR/DOC/2023/2016
44) MARTINEZ MARTINEZ, RICARD. “LOS TRATAMIENTOS DE DATOS PERSONALES EN LA CRISIS DELCOVID-19. UN ENFOQUE DESDE LA SALUD PÚBLICA”. Director de la Cátedra de privacidad y Transformación Digital Microsoft Universidad de Valencia. Diario La Ley, Nº 9601, Sección Doctrina, 25 de Marzo de 2020.
45) RETORTILLO BAQUER, LORENZO MARTIN. “LA CONFIGURACIÓN JURÍDICA DE LAADMINISTRACIÓN PUBLICA Y EL CONCEPTODE "DASEINSVORSORGE". Valladolid.
46) DIEZ SASTRE, SILVIA. “LA TÓPICA COMO MÉTODO EN EL DERECHO PÚBLICO”. Revista de Derecho Público: Teoría y Método Marcial Pons Ediciones Jurídicas y Sociales Vol. 1 | 2020 pp. 363-396 Madrid.
47) PERLO, CLAUDIA L. “APORTES DEL INTERACCIONISMO SIMBÓLICO A LAS TEORÍAS DE LA ORGANIZACIÓN”. Invenio, vol. 9, núm. 16, junio, 2006, pp. 89-107. Universidad del Centro Educativo Latinoamericano Rosario, Argentina.
48) ROMERO SILVERA, GRACIELA. “Interés público y protección de datos personales con especial referencia a los Derechos Humanos”. SEMINARIO REGIONAL DE PROTECCION DE DATOS. Montevideo, Uruguay, 1- 4 de junio de 2010.
49) CEJAS, EILEEN BERENICE Y GONZÁLEZ, CARLOS CÉSAR. “Estado de la normativa sobre video vigilancia en Argentina y su relación con la protección de datos personales”. SID 2015, 15º Simposio Argentino de Informática y Derecho. adfa, p. 1, 2011.©Springer-VerlagBerlin Heidelberg 2011.
50) ORDOÑEZ PIÑEDA, LUIS. “La protección de datos personales en lo sestados que conforman la Comunidad Andina: estudio comparado y precisiones para un modelo interamericano de integración”. Revista de Derecho, No. 27,ISSN 1390-2466 • UASB-E / CEN • Quito, 2017. En https://revistas.uasb.edu.ec/index.php/foro/article/view/502/489

51) SANTI PEREYRA, SILVANA ESTEFANÍA. "Biometría y vigilancia social en Sudamérica: Argentina como laboratorio regional de control migratorio". Rev. mex. cienc. polít.soc vol.63 no.232 Ciudad de México ene./abr. 2018. http://www.scielo.org.mx/scielo.php?pid=S0185191820180001002 47&script=sci_arttext.
52) SALTOR, CARLOS EDUARDO. "La Protección De Datos Personales: Estudio Comparativo Europa-América Con Especial Análisis De La Situación Argentina". memoria para optar al grado de doctor. Madrid, 2013.
53) FERNÁNDEZ GAZTEA, JOSEBA. "CONCEPTO Y FUNCIONES DE LA TÓPICAJURÍDICAEN EL DERECHO PÚBLICO". Revista de Derecho Público: Teoría y Método. Marcial Pons Ediciones Jurídicas y Sociales. Vol. 2 | 2020 pp. 51-72. Madrid, 2020.
54) GUEMES, CECILIA, "*Wish you were here*" confianza en la administración pública en Latinoamérica. Universidad Autónoma de Madrid / Departamento de Ciencia Política y Relaciones Internacionales, Madrid, España.
55) VILLAR PALASI, JOSE LUIS; VILLAR EXCURA, JOSE LUIS puesto al día por FERNANDEZ GARCIA, JUAN JESUS. "Principios de Derecho Administrativo". Tomo I. Conceptos y Fuentes. Universidad Complutense de Madrid. Facultad de Derecho. Madrid, 1987.
56) DEL TORO HUERTA, MAURICIO IVAN. "El fenómeno del *SoftLaw* y las nuevas perspectivas del Derecho Internacional" (pág. 514 a 549).
57) SARMIENTO, DANIEL. "La autoridad del derecho y la naturaleza del *SoftLaw*". Universidad Complutense de Madrid. Cuadernos de derecho público, núm. 28 (mayo-agosto 2006).
58) GEN DOHMANN, INDRA SPIECKER, "Instrumentos Estatales para la superación de los escenarios de incertidumbre y autorregulación". CAPITULO 2, (Pág. 48 a 311).
59) GORDILLO, AGUSTIN A. "Hacia la unidad del orden jurídico mundial". Capitulo XXII (pág. 2 a 48).
60) COLMEGNA, PABLO DAMIAN. "Impacto de las normas del *softlaw* en el desarrollo del derecho internacional de los derechos humanos". Revista electrónica del instituto de investigaciones "Ambrosio L. Gioja". Año VI, número 8, 2012. Facultad de Derecho. Universidad de Buenos Aires.
61) VILLAR PALAIS, JOSE LUIS. "La estructura peculiar del ordenamiento administrativo". (pág. 287 a 306).

62) CANDA, FABIÁN O. “El Derecho Administrativo, [2015] - (07/10/2015, nro. 13.828) [2015] Principios convencionales del procedimiento administrativo. El principio de "tutela administrativa efectiva". Creación y evolución en la jurisprudencia de la Corte Interamericana. Recepción en la jurisprudencia de la Corte Suprema nacional.
63) CASSESE, SABINO. “El espacio jurídico global” (E) RAP núm. 157. (pág. 11 a 26.
64) SABA, ROBERTO. (Des) igualdad Estructural, en Jorge Amaya (ed.), Visiones de la Constitución, 1853-2004, UCES, 2004, pp. 479-514.
65) PLUGOBOY, MATIAS A. “El derecho a la información Pública en Entre Ríos” en “Constitución de Entre Ríos. Logros y deudas a diez años de la Reforma Constitucional”. Director Andrés Manuel Marfil. Pág. 401 a 425. Ed. Delta Editora, año 2018.
66) MARFIL, ANDRES MANUEL. “Polémicas en los Procesos Constitucionales Urgentes a diez años de la reforma Constitucional Local” en “Constitución de Entre Ríos. Logros y deudas a diez años de la Reforma Constitucional”. Director Andrés Manuel Marfil. Pág. 333 a 399. Ed. Delta Editora, año 2018.

Jurisprudencia:

1) CAMARA CONTENCIOSO ADMINISTRATIVO FEDERAL- SALA V Expte. Nº 49.482/2016/CA1 “Torres Abad, Carmen c/ En-jgm s/ Habeas Data” Buenos Aires, julio de 2018. https://cpdp.defensoria.org.ar/wp-content/uploads/sites/4/2017/10/Fallo-Camara-Contencioso.pdf

2) CSJN. Fallo: 567/2021 “Gobierno de la Ciudad de Buenos Aires c/ Estado Nacional (Poder Ejecutivo Nacional) s/ acción declarativa de inconstitucionalidad”. Buenos Aires, mayo de 2021.

3) Tribunal de Distrito de La Haya “C / 09/550982 / HA ZA 18-388” [declara contrario al artículo 8 CEDH sistema *Systeem Risicoindicatie* (SyRI)]. La Haya, 05 de febrero de 2020. https://gdprhub.eu/index.php?title=Rb._Den_Haag_-_C/09/550982/HA_ZA_18/388.
El texto solo es accesible en inglés y neerlandés.

4) CSJN: “Halabi, Ernesto c/P.E.N. –ley 25.873 –dto. 1563/04 s/amparo ley 16.986”
Corte Suprema de Justicia de la Nación, 24 de febrero de 2009.

5) Tribunal Constitucional Español. “Federico Serna Vergara s/ Recurso de Amparo 4184-2000 c/ Ministerio del Interior”. SENTENCIA 14/2003, de 28 de enero (BOE núm. 43, de

19 de febrero de 2003)ECLI:ES:TC:2003:14. https://hj.tribunalconstitucional.es/HJ/es/Resolucion/Show/4789#ficha-tecnica

6) Sentencias del Tribunal Constitucional Federal de Alemania:
Caso BvR 256/08, BvR 236/08 y BvR 568/708. Sentencia de fecha 27.02.2008.
Caso 1BvR2835/17. Sentencia de fecha 19.05.2020.
En:https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2020/05/rs20200519_1bvr283517.html