Artículos libres

Smart contracts y protección de datos personales

Smart contracts and personal data protection

Flores, María Emiliana

María Emiliana Flores *
mariaemilianaflores@gmail.com
Universidad Nacional del Litoral, Argentina

PAPELES del Centro de Investigaciones de la Facultad de Ciencias Jurídicas y Sociales de la UNL
Universidad Nacional del Litoral, Argentina
ISSN: 1853-2845
ISSN-e: 2591-2852
Periodicidad: Semestral
vol. 15, núm. 26, e0009, 2023
papelesdelcentro@fcjs.unl.edu.ar

Recepción: 17 Septiembre 2022
Aprobación: 26 Abril 2023

URL: http://portal.amelica.org/ameli/journal/500/5004175009/

DOI: https://doi.org/10.14409/pc.2023.26.e0009

Resumen: *Blockchain* es una tecnología innovadora que permite hacer más eficiente la vida de las personas, a partir de un variado campo de acciones, que entre otras cosas permiten realizar transacciones que generan confianza y disminuir los gastos de operación. En relación con *Blockchain* surgen los *Smart Contracts*, produciendo una revolución en materia contractual. Existen grandes apuestas en torno a éstos avances tecnológicos para varios sectores como el financiero o el registral. No obstante, a pesar de los evidentes beneficios, se advierten algunos obstáculos al cumplimiento de las normas en materia de protección de datos personales en el servicio de los contratos inteligentes vinculados en específico al control de privacidad/ confidencialidad y al derecho al olvido por los principios regentes de *Blockchain*.

Palabras clave: contratos inteligentes, protección de datos personales, cadena de bloques.

Abstract: *Blockchain is an innovative technology that allows for a more efficient life for people, through a variety of actions, including enabling trustworthy transactions and reducing operating costs. In relation to Blockchain, Smart Contracts have emerged, revolutionizing the field of contracts. There are great expectations surrounding these technological advances for various sectors such as finance or registration. However, despite the obvious benefits, some obstacles are being identified regarding compliance with regulations on personal data protection in the service of smart contracts, specifically in relation to privacy/confidentiality controls and the right to be forgotten due to the governing principles of Blockchain.*

Keywords: *smart contracts*, *personal data protection*, *blockchain*.

1. Introducción

El derecho contractual tradicional se ha caracterizado por involucrar una serie de formalidades que afectan la celebración y la ejecución de los contratos. Con el avance de la tecnología y la globalización, el mundo contractual que previó Vélez comenzó a verse altamente modificado. Ante la nueva realidad subyacente, nuevas figuras contractuales y nuevas protecciones a los derechos surgieron.

Actualmente, nos encontramos frente a un paradigma disruptivo en materia tecnológica. *Blockchain, criptomonedas, Smart Contracts, tokens, NFT* son términos que comenzaron a aparecer en nuestras vidas. Como toda revolución, encontramos bandos contrapuestos – haters y fans - que han incursionado en éste nuevo mundo digital donde el *core* original han sido los desarrolladores.

Surge entonces, una nueva forma de contratación: *Smart Contracts* y el sector legal no puede resultar ajeno a dicho fenómeno, con el correlato de los nuevos desafíos jurídicos que ello traerá aparejado. Dados los principios en los que se erige la *Blockchain* y el resto de los nuevos paradigmas, cabe preguntarse ¿son compatibles con nuestra normativa?

Es importante recordar que el derecho debe estar en constante actualización para adaptarse o reinterpretarse y dar certeza a situaciones concretas ya que el mismo al fin y al cabo busca dar soluciones justas a problemas surgidos de la realidad histórica.

Por eso es completamente necesario que todos los operadores del derecho tomemos parte y mantengamos la posición que nos corresponde en el futuro tecnológico de la contratación electrónica y los *Smart Contracts*.

Es menester, precisar una definición de los llamados datos personales. Nuestro ordenamiento jurídico establece que los mismos son "Información de cualquier tipo referida a personas físicas o de existencia ideal, determinadas o determinables" y también define a los datos sensibles como "Datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual." Si bien es sabido que los segundos han sido tratados y protegidos con mayor amplitud, en el manejo de los datos personales radica la posibilidad de las personas de ejercer su derecho fundamental a la privacidad y el control sobre su información personal. Sin embargo, a los efectos del presente trabajo, todo lo desarrollado en vinculación con los datos personales puede ser pensado también en su aplicación a los datos sensibles.

2. Planteo de la problemática, objetivos generales y específicos

2.1. Planteamiento del problema

El cambio de paradigma tecnológico en el que estamos inmersos trae como nuevas figuras la *Blockchain* y los *Smarts Contracts* que poseen características que brindan seguridad a sus usuarios como la inmutabilidad y la transparencia.

Actualmente nos encontramos ante un gran avance en materia de protección de datos personales a nivel mundial donde diversos organismos buscan su protección y resulta de ello una normativa acorde. Argentina tiene pendiente su nueva ley de protección de datos personales pero la jurisprudencia ha sido armoniosa con las directrices establecidas por esos organismos a nivel mundial tomando figuras que no se encuentran legisladas en nuestro derecho como el derecho al olvido.

En este sentido, y como siempre ocurre ante un nuevo paradigma, debemos preguntarnos si estas nuevas figuras resultan acordes a nuestra normativa.

2.2. Objetivos Generales y Específicos

En cuanto a los objetivos, establecemos que el primero será el general y los consecuentes, los específicos:

- Analizar las problemáticas que se plantean en relación a los *Smart Contracts* y la protección de datos personales, comprendiendo los aspectos básicos tanto de la *Blockchain* como de los *Smart Contracts,* teniendo en mente los principios en los que se basan.
- Investigar diferentes posturas doctrinales y de organismos referentes de la materia para determinar si existe colisión normativa.
- Advertir el impacto presente y futuro del cambio de paradigma en la sociedad como en el derecho.
- Determinar la extensión de la problemática y encontrar una solución admisible.

2.3. Hipótesis

A causa de sus características de inmutabilidad y transparencia, los *Smart Contracts* ponen en peligro el control de privacidad y la correlativa protección de datos personales.

3. Estado Actual de la Materia

Es indudable la revolución tecnológica que se ocasionó con el acceso a internet desde el año 1993 cuando Estados Unidos levanta la prohibición respecto de la utilización de internet y deja de administrar de manera gubernamental la red, no solo en cuanto a nuevas tecnologías sino también en relación al comercio, la contratación electrónica y los medios electrónicos de pago.

En la actualidad, ha surgido una nueva tecnología que ha generado opiniones contrapuestas pero que nos ha traído nuevas aristas por resolver. Es la denominada *Blockchain*, una tecnología que responde al mecanismo "*distributed ledger techonoly*", construyendo una base de datos digital con criptografía. La también denominada "cadena de bloques" posee dos clasificaciones: privada (*permissioned*) y pública (*permissionless*). En palabras de Marcos Allende López y Vanessa Colina Unda: "(...) un registro descentralizado de información que se almacena en forma de transacciones que se agrupan en bloques."

Pudiendo concluir que "*Blockchain* puede definirse como el conjunto de tecnologías que, mediante el uso de técnicas criptográficas, consigue establecer un registro de información distribuida en red, sin que la validez de la información tenga que estar certificada por una autoridad central.

Consiste en un sistema digital de igual a igual o *peer to peer* (P2P), que permite la realización de transacciones verificadas sin intermediarios. Es la propia red, por consenso entre los participantes, la que garantiza que la información no ha sido alterada en forma alguna."

Dentro de los algoritmos de la *Blockchain*, encontramos a los *Smart Contracts*, término acuñado por Nick Szabo. Actualmente no hay uniformidad en si jurídicamente son contratos, existiendo quienes niegan su naturaleza contractual y quienes lo reconocen como un verdadero contrato. Teniendo en cuenta que el presente trabajo no tiene por fin determinarlo, ésta autora se adhiere a la postura afirmativa.

"Los *Smart-Contracts*, o contratos inteligentes, no son más que algoritmos almacenados en la *Blockchain* y que ejecutan decisiones automatizadas, es decir, se trata de un programa para ejecutar ciertas obligaciones pre-determinadas cuando se cumplen una serie de requisitos o situaciones previas de forma automática y sin necesidad de intervención humana en muchos casos."

A través de lo que se denomina oráculo que es una herramienta pactada por las partes previamente, se verifica el cumplimiento de las condiciones pautadas en el contrato, ejecutando las prestaciones automáticamente mediante códigos informáticos.

Los *Smart Contracts* poseen dos características que devienen propias por su utilización de la *Blockchain* que son la inmutabilidad y transparencia, haciéndolos seguros y confiables ya que el riesgo de manipulación y falsificación es bajo. En *Ethereum* por ejemplo, los contratos almacenan en la *Blockchain* el código ejecutable del programa, los datos asociados a él y el balance del contrato. Al igual que las cuentas de los usuarios tienen una dirección, los contratos también la tienen, pudiendo ejecutar funciones o transferir fondos. Motivo por el cual se sostiene que las transacciones u operaciones que se realizan en la *Blockchain* no son confidenciales, ya que todo individuo que tenga acceso a la cadena de bloques, puede acceder y ver toda la información que se envía y se almacena en un contrato. Aunque una de las ventajas de esta revolucionaria tecnología es la transparencia, en estos casos puede ser un inconveniente.

3.1. Problemática con la protección de datos personales

Las mayores problemáticas en torno a la protección de datos personales ocasionadas con el surgimiento de los *Smart Contracts* que el Derecho necesita dar respuesta son, al entender de ésta autora, por un lado, la ocultación de la identidad personal, y por el otro, la protección de datos de carácter personal. Sumado a ello, se encuentra en tensión la legislación en torno al Derecho al Olvido. Podemos señalar que los dos primeros problemas se vieron parcialmente resueltos con la encriptación de datos y acompañados de una normativa (en el caso de Europa) de protección de datos.

Tomando como base el *GDPR* en el que ahondaremos más adelante, podemos mencionar el amplio debate en torno a las posibles incompatibilidades del mismo con el uso de la tecnología *Blockchain*, trasladable a los *Smart Contracts*. Entre las cuestiones que plantean controversia se encuentran:

Identificación de actores: El *GDPR* impone obligaciones y responsabilidades a los diferentes actores involucrados en el tratamiento de datos personales, lo que hace necesario identificar la posición jurídica de cada uno de ellos. Sin embargo, esto puede resultar complicado en la tecnología *Blockchain*, donde cada actor de la red tiene acceso a los datos personales y resulta difícil determinar quién es el responsable y el encargado del tratamiento. Esta cuestión no es pacífica y se encuentra en debate entre las autoridades de protección de datos y los grupos de trabajo especializados en Europa. Una posible solución es operar en una red *Blockchain* privada, en la que los propietarios deciden quién puede participar en la misma y se puede identificar mejor el rol de cada actor en la protección de datos.

Ejercicio de derechos, rectificación o supresión: El derecho de supresión y el de rectificación plantean dudas en cuanto a su aplicación en la tecnología

Blockchain, que es por naturaleza inmutable. Una posible solución es aplicar procesos de anonimización irreversibles, de modo que el dato sea tan inaccesible que pudiera equivaler a la supresión del mismo. En cuanto a la rectificación, se podría introducir un nuevo registro que modifique el anterior, siendo el último el valido.

Toma de decisiones automatizadas con efectos jurídicos: El uso de smart contracts implica la automatización de decisiones, lo que puede resultar contrario al RGPD. Sin embargo, la versatilidad de la tecnología Blockchain permitirá que dichos contratos inteligentes puedan ser configurados y adaptados para cumplir con la exigencia de la intervención humana.

Otros aspectos a tener en cuenta: se debe analizar detenidamente la base legitimadora que es de aplicación a cada caso y la relación entre los diferentes actores de la red *Blockchain*. La participación de actores en diferentes lugares del mundo en un sistema basado en *Blockchain* podría suponer la existencia de transferencias internacionales de datos que, en su caso, sería necesario regular. Además, los datos personales incorporados en *Blockchain* deberían estar anonimizados para disminuir el impacto en los derechos y libertades de los interesados

3.2. Confidencialidad/ Privacidad

Éste conflicto surge ante la característica propia de transparencia, que si bien resulta positiva para evitar actos fraudulentos, manipulación, falsificación o para la generación de confianza y seguridad, podemos analizarlo como algo negativo si las partes, por ejemplo, buscan la confidencialidad de la existencia del contrato o la privacidad de sus cláusulas –aun con la existencia de cláusulas de confidencialidad-.

Puede lograrse en el caso de utilizar un servidor privado pero "en el caso de la utilización de plataformas DLT públicas, la información puede estar potencialmente al alcance de los diferentes participantes/usuarios de la plataforma, o del operador de ésta, aunque sometido a los términos y condiciones de uso. Mantener la confidencialidad requeriría la restricción de los accesos a la información o, por lo menos, intentar garantizar el anonimato de la información relevante mediante técnicas de encriptación, por ejemplo. En cualquier caso, siempre existirá un cierto nivel de tensión e incertidumbre al utilizar plataformas abiertas, dada la incertidumbre y las potenciales vulnerabilidades a las que se los usuarios se exponen."

3.3. Derecho al Olvido

Otra arista y más controvertida es la que afirma que la tecnología en la que se apoyan los *Smart Contracts, Blockchain* es contraria a la normativa de Protección de Datos.

"Entre los derechos reconocidos por nuestra normativa se encuentra la obligación del responsable del tratamiento de datos de borrar o rectificar datos personales cuando un interesado lo solicite. Pues bien, esta posibilidad de modificar o suprimir datos, es la que puede generar mayores problemas entre

la normativa de protección de datos y *Blockchain*. El motivo es que hay un choque frontal entre el derecho a la modificación o supresión de los datos y la inalterabilidad e inmutabilidad del dato en *Blockchain*."

Es menester señalar que el derecho al olvido no está explícitamente legislado pero la doctrina y jurisprudencia argentina han ido definiéndolo entendiendo que luego de un determinado espacio de tiempo hay ciertas informaciones que deben ser eliminadas y evitar así que el individuo quede prisionero de su pasado. En Europa, por su parte, los debates han sido también muy candentes previo al dictado de la GDPR.

El derecho al olvido tiene íntima relación con el habeas data y fue la ley 25.326 que permitió a la jurisprudencia delinear el derecho al olvido en los fallos Catania y Napoli guiándose en los artículos 16 y 26 de dicha ley. Es por ello que la doctrina nacional ha aseverado que nuestro país está en "camino a una armonización de normativa y estándares con la Unión Europea".

4. Marco Fáctico, Socio-Económico

Luego de las aclaraciones anteriores, es primordial establecer las implementaciones existentes de *Smart Contracts* en términos generales y su consecuente impacto factico socio-económico, a saber:

Son completamente útiles para llevar un registro en las etapas de desarrollo de un producto. Si las partes determinan la realización de pagos al finalizar alguna fase, por ejemplo, una vez alcanzada el contrato libera la transferencia.

Los *Smart Contracts* se han utilizado en *ICOs .Inicial Coin Offers*) y han tenido una relevancia importante por las implicaciones que está teniendo. Las *ICOs* se rigen con un *Smart Contract* en el que instituyen las reglas para la adquisición de la nueva moneda y gestionan de forma automática la emisión y compra de la misma.

Es el sector financiero el que resulta más compatible con las innovaciones tecnológicas y digitales puesto que generalmente sus activos ya se encuentran digitalizados, resultándole más sencillo adaptarse a los cambios.

Siguiendo con ésta línea de pensamiento, "los actores principales que podrían beneficiarse de la tecnología *Blockchain* son (entre otros) los bancos y mercados financieros, ya que podrían reducir costes, seguirían siendo seguros y más eficientes. Con *Ethereum* se podrían crear aplicaciones que funcionen de manera descentralizada y que usen los *Smart Contracts* para desarrollar sus funciones."

Se puede mencionar como ejemplo España, donde, si por causa atribuible a la aerolínea hay un retraso en la hora de salida del avión establecida en el boleto, el pasajero tiene derecho a un reembolso del 7% del valor de su pasaje. Si la compra se efectuó a través de un contrato inteligente, bastará con la verificación de la demora por la torre de control para que el dinero se deposite en tiempo real en la cuenta del pasajero. Otro caso es Toyota, que por su parte, está probando su implementación en la venta de automóviles en cuotas. De esta manera, la falta de pago en tiempo de la cuota del automotor recientemente adquirido hace que, de manera instantánea, una orden se ejecute desde algún lugar remoto del mundo, produciendo la inmediata detención del vehículo, esté donde esté, hasta tanto no se verifique el pago de los montos adeudados.

Ejemplos generales de implementación de *Smart Contracts* son: venta de productos de internet, registro de patentes, trazabilidad alimentaria, seguros, ventas de productos, alquileres y hoy existe su utilización en realidades virtuales, donde un claro ejemplo es Descentraland.

Es correcto afirmar que la *Blockchain* instauró una nueva manera de realizar transacciones, mejorando la repartición del capital global y otorgando mayores oportunidades. Ello representa un cambio en el sistema financiero global, dada la revolución del modelo económico actual. *Blockchain* es una tecnología que definitivamente llegó para quedarse y que no pasa desapercibida.

"Actualmente, vivimos en una época de era digital, donde la innovación supone una revolución para todos, además, el mundo necesita producir, gestionar y almacenar una enorme cantidad de información certificada en todo momento, que hasta ahora han hecho humanos. Mediante el avance tecnológico, hemos cambiado las maneras de hacer las cosas, que hasta este momento era una rutina"

Para utilizar un *Smart Contract*, lo primero que debe analizarse es si las cláusulas del contrato pueden transcribirse a código. Si ello es posible, hay distintos smart contracts que se pueden configurar, como por ejemplo alquileres y compraventa. En el primero, uno de los beneficios seria que se evita que las partes modifiquen el contrato. En el segundo, la ventaja latente es el ahorro en costes notariales pudiendo verificar el cambio de titularidad a través de firma digital. También puede aplicarse –tal como lo hacen las Universidad Carlos III y UNIR de España- para evitarlas falsificaciones de documentos tales como diplomas universitarios. Todo lo descripto lo permite una característica esencial de la *Blockchain*: la inmutabilidad, es decir, los datos ingresados a la cadena de bloques no son a priori modificables. No debemos olvidar que otra de las características que hace tan atractivo a los *Smart Contracts* es la eliminación de intermediarios y/o terceros. De esta manera, la posibilidad de que un ajeno modifique el documento a su favor también se encontraría eliminada. Es por ello que, a causa de las propiedades de inmutabilidad y transparencia propia de la red, los contratos inteligentes representan una revolución.

En palabras de la Daniela B. Valentini: "Con el uso de los contratos inteligentes se pueden realizar tareas cada vez más complejas, simplificando y automatizando todo tipo de procedimientos. Así, *Blockchain* podría ser más que un registro y comenzar a pensarse en el uso de smart contracts en procesos como sistemas de trazabilidad de productos, de emisión de documentos, incluso para configurar actuaciones administrativas automatizadas, en procedimientos de licitación y contratación pública, evaluación de ofertas (aplicando de forma automática los criterios reglados y parametrizados que se establecen en el Pliego), subvenciones y subsidios, ingreso de pagos, entre otras."

Valentini ejemplifica diferentes iniciativas donde ostentan los beneficios de la utilización de la *Blockchain* y *smart contracts*. Podemos citar el caso de las empresas *Maersk Line* e *IBM* en el sector del transporte y la logística, donde tienen como objetivo la trazabilidad, buscan lograr transparencia y seguridad de punta a punta y en tiempo real a la cadena de suministro. La misma intención fue la de *Wal-Mart* cuando exigió a sus proveedores para antes de septiembre del 2019 utilizar el software desarrollado por *IBM*. En Rusia y en particular el sector minero, con el propósito de asegurar la autenticidad de la cadena de suministro, utiliza la tecnología *Blockchain* para el rastreo de diamantes naturales, desde la

extracción y el pulido hasta que llegue al consumidor final. Otros países que indagan en la cadena de bloques son, Brasil, Emiratos Árabes Unidos y China, con la finalidad de implementar un sistema de gestión de residuos sólidos domésticos. También, como ya se mencionó, algunas universidades la utilizan para evitar títulos falsificados.

Pero, lo cierto es que materialmente, los Smart Contracts utilizan una tecnología innovadora que actualmente está implementándose en países del primer mundo en su vida cotidiana. Argentina se encuentra en crecimiento dentro de la materia a nivel regional y hay mucho talento nacional involucrado en este tipo de desarrollo en todo el mundo. Es así como existen compañías, en su mayoría pertenecientes al sector financiero, que se encuentran implementando contratos inteligentes como *RSK, Koibank* y *RUS*. Sin embargo, fuera del sector en apogeo y en el público en general el porcentaje de personas conocedoras de estas scripts es reducido, produciendo desinformación acerca de su aplicabilidad y de los problemas que pueden suscitarse. En particular, con nuestra problemática, a nivel mundial hay todavía mucho que resolver: definiciones, naturaleza jurídica, colisión normativa, postura judicial. Lo cierto es que hay distintos organismos y doctrinarios preocupados con la protección de datos personales en contratos inteligentes y *Blockchain* pero todavía no se ha suscitado ningún pleito en donde pueda profundizarse el meollo de la problemática. No así, con el caso de los criptoactivos donde si encontramos más adeptos con conocimientos en la temática como también aquellos quienes los adquieren sin conocimiento alguno y donde podemos encontrar por ejemplo, empresas multadas como el caso de *Tether*.

5. Estudio de Doctrina

La doctrina nacional como internacional se ha ocupado de intentar definir a los contratos inteligentes, analizar su naturaleza jurídica y sus elementos pero son muy pocos los que han tratado la problemática de protección de datos personales y *Smart Contracts*.

Sin embargo, es preciso hablar de los problemas que la doctrina ha escrito para poder razonar el problema planteado en el presente trabajo.

Cristina Poncibo explica por su parte cuando un contrato inteligente puede considerarse contrato en sentido jurídico ya que deben concurrir ciertas circunstancias. Agrega que la doctrina europea y americana discuten sobre la validez del *Smart Contract*, explayándose en que son los estudiosos del common law que parecen más propensos a admitir la posibilidad de que tal programa pueda configurar un contrato propiamente dicho, puesto que el consentimiento de las partes puede expresarse sin especiales formalidades, al negociarse el contrato utilizando un medio digital. No opinan lo mismo los colegas de Europa continental (p. ej., Alemania, Francia, Italia y España), que manifiestan una mayor prudencia al considerar que el smart contract no puede llegar a ser un verdadero contrato, sino solamente representar un mero hecho ejecutivo de un contrato.

Por su parte, Nicolás Negri desarrolla la postura de Eliza Mik quien habla de programas que se ejecutan en la *blockchain* y no de contratos en un sentido jurídico e incluso critica el antecedente establecido por Szabo de las máquinas

expendedoras como antecedentes de los contratos inteligentes. Negri también plantea otra visión menos critica como la de Arcari quien ha definido a los contratos inteligentes como el código de un programa de computación que automatiza la verificación, la ejecución y el cumplimiento de ciertos términos y condiciones de un contrato. Para Arcari, los contratos inteligentes son acuerdos automatizados, que hacen depender el cumplimiento del contrato del acaecimiento o no de ciertas condiciones objetivas, predeterminadas en el código de programación de aquellos, de acuerdo con lo pactado en un contrato.

También acerca la definición que para éste autor es la más acertada y que otros doctrinarios adhieren y es la de Tur Fernández "aquellos contratos celebrados a través de una página web accesible para las partes cuya forma está constituida por la interfaz de usuario de la aplicación externa y uno o varios programas autoejecutables (*smart contracts*) residentes en la cadena de bloques con capacidad para interactuar recíprocamente y con dicha interfaz".

Negri también acerca las categorías que proponen El Observatorio y Foro de Blockchain de la Unión Europea en 1-Smart Legal Contracts y 2- Smart Contracts con implicancias legales. Otra clasificación propuesta es 1- Suaves y 2- Puros.

Santiago Mora hace una mención sobre la problemática planteada en éste trabajo cuando advierte que "se pueden generar problemas en materia de privacidad y confidencialidad de la información en general, y en particular en relación con la configuración de los derechos de acceso, supresión, actualización y modificación."

Siguiendo a Arcari, los *Smart Contracts* comparten con los contratos convencionales el término privacidad bajo el principio general del derecho: efecto relativo de los contratos. Pero, amplían el término privacidad ya que involucra la privacidad de identidad y transacción de las partes.

Sebastián Heredia Querro, entiende que éstas últimas están intrínsecamente ligadas al control y la confidencialidad, pero también a las formas especiales de identidad -anónima y seudónima- que permite la cadena de bloques.

Siguiendo con éste autor, se explica que en cuanto a la privacidad del contrato, si bien las partes controlan el contrato, el problema radica en que el código del contrato es públicamente visible –si hablamos de una blockchain pública- y por ello, el contrato no es ni será confidencial.

Todas las *blockchains* permiten justamente dejar un registro y asociar tales transacciones a las llaves públicas entre las cuales tuvieron lugar –estas no son necesariamente conocidas por todo el mundo. Por tanto, es técnicamente más correcto hablar de pseudonimidad. Los desarrollos de encriptado asimétrico no son nuevos, y son una característica esencial de todas las *blockchains* públicas. Es la tecnología que permite que la identidad real de un usuario de blockchain sea protegida, del mismo modo que se protegen los números de una tarjeta de crédito cuando se hace una compra online a través de una línea no segura.

En *blockchain*, la privacidad se consigue de tres modos: operando anónimamente; encriptando la información; y no alojando información sensible en una *blockchain*, sino en canales paralelos *of-chain*. Ésta idea es muy importante mantenerla en mente para la posibilidad de instaurar una solución a nuestro problema.

En la actualidad, surgieron distintas empresas que ofrecen la posibilidad de dificultar la vinculación de identidad a una llave pública cómo aquellas que hacen lo contrario, buscan asociar la identidad con la llave pública correspondiente. Existe otro recurso en el cual por cada transacción, se crea una nueva llave pública, de ésta manera se dificulta el seguimiento de la identidad del usuario. Por último, es necesario mencionar a las *On-ChainAnalysis*, un método emergente en el que se observan los datos públicos de transacciones registrados en la *blockchain* y si se suman los *Smart Contracts* que se utilizan para dichas transacciones, se pueden extraer patrones de quién, cómo y cuándo utiliza criptomonedas.

Por su parte, Marcelino Tamargo, sostiene que la *CNIL .Comisión nacionales de l´informatique et des libertés*) autoridad francesa de protección de datos personales es la primera autoridad europea en la materia en pronunciarse sobre la compatibilidad de ésta tecnología con la protección de datos personales, tal y como está regulada en la normativa existente. La realidad es que la finalidad buscada por la normativa como por la *blockchain* es la misma: más control al individuo sobre el tratamiento de sus datos personales pero con distinto enfoque y es precisamente en ésta dicotomía donde se genera el potencial conflicto ya que por un lado, la normativa europea se rige por un sistema centralizado haciendo foco en el responsable del tratamiento de datos personales de la organización quien tiene un control absoluto de los mismo pudiendo acceder, modificar o suprimirlos. Por el otro lado, tenemos a la blockchain con una lógica contrapuesta ya que se basa en la descentralización de su gestión, donde no se pueden alterar los datos sin que afecte a la cadena de bloques.

Basándose en el art. 25 del *GDPR*, la *CNIL*, recomienda que la *blockchain* solo se emplee cuando sea necesario. Propone reducir los datos personales únicamente a la clave pública y de ser necesario ingresar más datos personales a la cadena de datos, se necesitará tomar medidas adicionales para garantizar máxima confidencialidad. Por último, entiende que urge una regulación más específica de la normativa para facilitar el tratamiento de datos en la *blockchain*.

Elvira Sebastià Puig señala que es la colisión entre la naturaleza de la tecnología empleada en los contratos inteligentes y la regulación actual de protección de datos personales –en particular *GDPR-* la razón por la que se genera el conflicto existente entre la materia de protección de datos y los *Smart Contracts*. La normativa del *GDPR* se manifiesta como una autentica declaración de derechos fundamentales de protección de datos en el ámbito digital pero la nueva tecnología tiene preceptos contrarios. Algunos de los problemas radican en: por un lado el *GDPR* define dato personal como "cualquier información relativa a una persona física viva identificada o identificable" y dado que la IP permite identificar el equipo que ha tenido acceso a internet, la Agencia Española de Protección de Datos como el Tribunal Supremo han declarado su postura de que se trata de un dato personal. Y siendo consecuente con el razonamiento, los *Smart Contracts* utilizan *blockchain*, y si bien en ella no se utilizan datos personales cada vez que se accede a la cadena, sí quedan registradas las entradas y salidas en cada transacción efectuada. De este modo, existiría la posibilidad de identificar al propietario de la conexión.

Por otro lado, la normativa de protección de datos establece la figura de un responsable del tratamiento de datos a quien le atribuye la responsabilidad de asegurar la efectividad de la normativa de protección de datos y es quien

responde en caso de incumplimiento. El usuario puede ejercer sus derechos ante él. En cambio, en la *blockchain*, todos los participantes tienen el control de cada transacción ya que es una red entre pares y su naturaleza es la descentralización por lo que no existe un responsable de tratamiento de datos.

Otra problemática radica en que el *GDPR* contempla en su texto una serie de derechos que se confieren a los usuarios cuyos datos están siendo tratados que son contrarios a los principios de la *Blockchain*. Por ejemplo, en el artículo 17 el *GDPR* recoge que los interesados tienen la posibilidad de solicitar al responsable del tratamiento la supresión de sus datos en una serie de situaciones que el texto contempla. Pero, el empleo de la cadena de bloques supone, por un lado, la inexistencia de un responsable del tratamiento tal como lo mencionamos anteriormente. Por otro lado, uno de los propósitos fundamentales del empleo del Blockchain es la inmutabilidad. Aquí se observa la colisión con la normativa del *GDPR*.

En último lugar, se encuentra el derecho a la limitación del tratamiento. De ésta manera, el interesado puede solicitar al designado responsable del tratamiento que se apliquen diversas medidas sobre sus datos para evitar su modificación, borrado o supresión. Nuevamente, éste derecho resulta incompatible con la inmutabilidad de los datos dentro de *Blockchain*. Ello, porque ésta tecnología se asienta en la creación de una base de datos imborrables.

6. Marco Normativo

6.1. Legislación Argentina

En miras de la normativa existente, es importante destacar, por un lado la relacionada con protección de datos personales y, por el otro, sobre *Smart Contracts*. En relación a la protección de datos personales, nos referimos primeramente a nuestra Carta Magna, ya que en el año 1994 se incorporó en el artículo 43, tercer párrafo, la acción de habeas datas donde se encuentra garantizado éste derecho manifestando que "...toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquéllos. No podrá afectarse el secreto de las fuentes de información periodística".

"Este hito regulatorio implicó la incorporación a nuestro texto ius fundamental del derecho a la protección de datos personales, desde su faz sustancial como procesal, lo cual se derivó en su ulterior recepción legislativa específica".

En el año 2000, se sancionó la Ley Nº 25.326 de Protección de Datos Personales, siendo una norma de orden público que regula los principios aplicables en la materia, así como también el procedimiento de la acción de habeas data, entrando en vigencia al año siguiente.

Sin embargo, en innegable afirmar que el escenario en el que la Ley N° 25.326 fue sancionada ha cambiado drásticamente en los últimos veintidós años dado la evolución tecnológica en los que estamos inmersos y que ha resultado de gran impacto en la protección de datos personales, generando nuevos interrogantes

legales y desafíos en el campo del ejercicio de los derechos. Como toda nueva realidad tecnológica los beneficios son celebrados con entusiasmo y aún más cuando se generan cambio de paradigmas, pero no hay que olvidar localizar, analizar e investigarlas nuevas potenciales vulneraciones a la privacidad para poder encontrar soluciones.

La entones DNPDP, dependiente del Ministerio de Justicia y Derechos Humanos, bajo el programa "Justicia 2020", tomo la iniciativa de confeccionar un proyecto de ley de protección de datos personales para reformar la normativa vigente y dar nacimiento a nuevos institutos, definiciones y reglas novedosas y altamente debatidas en la materia.

Siguiendo el mensaje de 147/2018, la nueva normativa tiene como premisa no ser un impedimento para la innovación y el desarrollo tecnológico y, al mismo tiempo, cumplir con los estándares internacionales, cuyo destino es la protección de datos personales y la privacidad. A lo largo de su articulado, éste proyecto, "garantiza adecuadamente los derechos de los titulares de los datos, aclara cuáles son las bases legales para el tratamiento de datos (incorporando al interés legítimo del responsable del tratamiento, entre otras bases legales, y alejándose de la ley vigente que únicamente contempla al consentimiento del titular de los datos) y genera obligaciones a los responsables del tratamiento de datos que son consistentes con el objeto de la norma proyectada: la protección integral de los datos personales a fin de garantizar el ejercicio pleno de los derechos de sus titulares." Proyecto de ley que generó expectativas pero que en su redacción encontramos incontables falencias.

Sumado a ello, el 25 de mayo del 2018 entró en vigencia el *General Data Protection Regulation* (GDPR o RGPD acorde a sus siglas en español), estableciéndose un nuevo contexto regulatorio internacional en esta materia y a la cual Argentina debe tener en cuenta como parte de la comunidad internacional.

En cuanto a las novedades introducidas por el proyecto de ley y concernientes al presente trabajo se puede mencionar: art. 2 donde define por un lado datos personales, estableciendo que se entiende por persona determinada, persona determinable, datos biométricos y datos genéticos y por el otro, define datos sensibles. El art. 16 habla de las excepciones del tratamiento de datos sensibles. Del art. 5 al 10 se establecen los siguientes principios: de lealtad y transparencia, de responsabilidad proactiva, de finalidad, de minimación de datos, de exactitud y el plazo de conservación. El art. 11 trata la licitud del tratamiento de datos, el 12 el consentimiento y el 14 las excepciones al consentimiento previo. El art. 15 manifiesta la información al titular de los datos. El art. 19 establece otro principio que es el de seguridad de los datos personales y lo refuerza con el art. 20 que habla de la notificación de incidentes de seguridad. El art. 21 establece el deber de confidencialidad. Del 23 al 25 trata sobre la transferencia internacional de datos personales. Del art. 27 al 33 se establecen los derechos del titular de datos personales. Las obligaciones del responsable y encargado del tratamiento de datos personales se instituyen desde el art. 37 al 45.

Una vez realizado la anterior mención de los articulados en materia de protección de datos concernientes al presente trabajo, queda analizar cómo se integrarían los contratos inteligentes a la legislación nacional de protección de datos personales contenida en la Leyes Nº 25.326, 27.275, 27.483y en Resoluciones dictadas por la autoridad de aplicación del régimen, como la

Resolución 4/2019. Entendemos que hay algunos supuestos en donde los *Smart Contracts* entran en colisión con la legislación en protección de datos quedando como alternativas o la adaptación de los *Smart Contracts* con nuestra legislación o nuestra legislación con la inmutabilidad de la *Blockchain*.

El derecho al olvido tiene intima vinculación con el habeas data, siendo una nueva institución jurídica "para poder lograr efectivamente, en un Estado de Derecho, la protección, seguridad, exactitud o rectificación, preservación o destrucción justificadas del secreto o privacidad sobre los datos del ciudadano, que el Estado u otros entes públicos o privados tengan sobre ellos con el propósito del conocimiento y difusión permitidos de los mismos, ya sea que estén archivados o guardados en medios electrónicos o similares, porque ellos constituyen testimonios o proyecciones de la persona, de la vida, de la identidad, pensamiento cultural o instrucción, actividades sociales, económicas, religiosas, así como los de la genética, salud, orientación sexual, pensamiento político, sea que ya se hallen registrados o por registrarse, según el amparo y protección que la Constitución y las Leyes respectivas ordenen."

Tal como se explicó al inicio, en nuestro ordenamiento jurídico el derecho al olvido no se encuentra legislado. Sin embargo, tanto la doctrina como la jurisprudencia de nuestro país han ido definiéndolo.

El derecho al olvido tiene íntima relación con el habeas data y la ley 25.326 permitió a la jurisprudencia proyectar el derecho al olvido en los fallos Catania y Napoli, donde en ambos casos mediante una acción de habeas date se pretendía borrar información sobre deudas bancarias guiándose en los artículos 16 – derecho de rectificación, actualización o supresión- y 26 – prestación de servicios de información crediticia-de dicha ley. Es por ello que la doctrina nacional ha aseverado que nuestro país está en "camino a una armonización de normativa y estándares con la Unión Europea"

Ejemplo de ello es el fallo argentino "Denegri, Natalia Ruth c/ Google Inc. s/ Derechos Personalísimos: Acciones Relacionadas" del año 2020 donde se ha reconocido expresamente el derecho al olvido tomando como eje el caso español Costeja, donde el Tribunal condenó a *Google* a cumplimentar con el derecho al olvido que se encuentra vigente en Europa. Éste fallo es de vital importancia ya que si bien podemos discutir acerca de la correcta aplicación del instituto, es el primer fallo argentino que reconoce expresamente el derecho al olvido.

No hay que olvidar señalar que el proyecto de nueva ley de datos personales, en su art. 31 también lo regula como Derecho de Supresión. En el mensaje de elevación de la norma proyectada, se señala que el derecho al olvido "ha traído muchas discusiones teóricas y críticas sobre su aplicación en la práctica, dado que una deficiente implementación podría devenir en violaciones a otros derechos fundamentales, como la libertad de expresión o el acceso a la información. De allí que en la propuesta que se somete a consideración, si bien se reconoce este derecho, se ha aclarado especialmente que el derecho de supresión no procede cuando el tratamiento de datos persiga un fin público o sea necesario para ejercer el derecho a la libertad de expresión e información."

Por su parte, la ley 27.275 trata el acceso a la información pública que es reconocido como un derecho fundamental. En su artículo 19 crea la Agencia de Acceso a la información pública como ente autárquico que funciona con autonomía funcional en el ámbito de la Jefatura de Gabinete del ministerio. Ésta

agencia fue designada Autoridad de Aplicación de la ley 25.326 de protección de datos personales.

En la ley 27.483 se aprobó el Convenio para la Protección de las personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal del año 1981 y posee un protocolo adicional al Convenio antes mencionado, a las autoridades de control y al flujo fronterizo de datos, suscripto en el año 2001.

Y para finalizar con la normativa argentina, no se puede dejar de mencionar el Criterio 2 de la Resolución 4/2019 que contiene los llamados criterios orientadores e indicadores de mejores prácticas en la aplicación de la Ley de Protección de Datos Personales. "Criterio 2. Tratamiento automatizado de datos. En caso que el responsable de la base de datos tome decisiones basadas únicamente en el tratamiento automatizado de datos que le produzcan al titular de los datos efectos jurídicos perniciosos o lo afecten significativamente de forma negativa, el titular de los datos tendrá# derecho a solicitar al responsable de la base de datos una explicación sobre la lógica aplicada en aquella decisión, de conformidad con el art. 15, inciso 1 de la Ley Nº 25.326." La naturaleza de los *Smart Contracts* radica en la toma de decisiones automáticas basadas en datos, lo cual ocurrirá siempre que exista un contrato inteligente, por lo que no resulta coherente que el titular tenga derecho recibir una explicación sobre la lógica de la decisión del contrato inteligente ya que habrá sido informado apropiadamente antes de iniciar el *Smart Contract*.

Es esencial destacar que nuestro ordenamiento jurídico no posee normativa específica sobre *Smart Contracts* y que mayoritariamente la doctrina entiende que se pueden aplicar las normas sobre contratos en general. Pero no debería acotarse allí ya que hay un sinnúmeros de situaciones que podrían suscitarse por lo que también le pueden ser aplicables las normas relacionadas a los contratos de adhesión, las relativas a la protección de datos personales, delitos informáticos, la legislación sobre defensa al consumidor.

No se debe confundir a los *Smart Contracts* con los contratos electrónicos, regulados en el art. 1105 del Código Civil y Comercial.

Los contratos electrónicos son aquellos que se llevan a cabo mediante medios electrónicos en donde el consentimiento o asentimiento se manifiesta exclusivamente por medios electrónicos y donde la ejecución de sus cláusulas depende del impulso de cada una de las partes.

Por su parte, los *Smart Contracts*, mediante el uso de tecnología *Blockchain* permite su ejecución de carácter automático sin intervención de un tercero para desencadenar sus consecuencias.

Siguiendo a Gianfelici, la ausencia de normativa sobre contratos inteligentes no impide la aplicación analógica del régimen propio de los contratos tradicionales respecto a la necesidad de existencia de consentimiento, objeto y causa.

Adelantándose, hay que prever de seguir los lineamientos que han dado el Observatorio y Foro Europeo sobre *Blockchain* ante la posibilidad de una futura regulación específica sobre la materia. En los lineamientos mencionados hay tres características relevantes; trabajo en conjunto del regulador con el sector privado, advertir los supuestos en donde se usen masivamente *Smart Contracts* y establecer pautas mínimas que sirvan para determinar la legislación y la jurisdicción aplicable.

6.2. Legislación Comparada

A la hora de analizar el derecho comparado hay que diferenciar de igual manera, la regulación de *Smart Contracts* por un lado y la de protección de datos personales por el otro.

Siendo los *Smart Contracts* sumamente novedosos a nivel global, ocurre que su validez es incierta jurídicamente y la normativa específica sobre la temática es muy reducida un número limitado de países, aun cuando se han desarrollado múltiples plataformas basadas en *Blockchain* que ofrecen la utilización de *Smart Contracts.*

Hay que entender que los *Smart Contracts* no pueden operar sin la *Blockchain*, razón por la cual muchas de las legislaciones que han abordado su regulación la han incorporado en su definición y tratamiento legal.

El principal interés en el derecho comparado comienza con los países que poseen el sistema del *Common Law* ya que han sido los primeros en afrontar la regulación, en especial Estados Unidos, buscando dar soluciones jurídicas ante la inexistencia de normativa que se acople a los *Smart Contracts*. Como estados pioneros en ésta temática podemos nombrar a Arizona y Vermont.

El primer estado del mundo en adoptar en su normativa la nueva tendencia tecnológica de cadenas de bloques fue Arizona, en 2017 cuando se aprobó la HB2417 en la Cámara de Representantes. En la mencionada normativa encontramos una definición legal sobre *Blockchain* y los *Smart Contracts*. En relación a éstos últimos la ley los considera legal, efectivo y válido ya que existen en el comercio.La ley específica que tanto una firma, como un registro o contrato que esté asegurado por medio de *blockchain* debe ser considerado legalmente en su forma electrónica, como los son las firmas o registros digitales.

En 2015, Vermont fue el primer estado en regular a la *Blockchain* y en mayo de 2018 a través del Act 269, se incluyó la definición de contrato inteligente que fue muy similar a la de Arizona. La novedad fue la introducción la *BBLLC*, ello es la denominación legal de sociedad de responsabilidad limitada basada en *Blockchain*. Ello está dirigido específicamente a aquellas compañías que operan un negocio utilizando la cadena de bloques en todo o parte de sus actividades. De esta manera se instauró la primera norma en la que se plantea un modelo sin intermediarios en la toma de decisiones de la sociedad. Otro punto novedoso de la ley es que se admiten los registros digitales existentes en la *Blockchain* como prueba admisible en juicio, siempre y cuando haya una declaración jurada de una persona autorizada a la entrada de los datos en la *Blockchain*.

Delaware es el estado denominado como la "cuna" del Derecho corporativos y donde se encuentran establecidas más de dos tercios de las compañías Fortune 500. Aquí se introdujo la SB 69 donde se les permite a las sociedades privadas constituidas en el Estado emitir y realizar un seguimiento de las acciones, accionistas y otros aspectos corporativos haciendo uso de la *Blockchain*. En éste caso, los *Smart Contracts* son empleados con finalidad jurídica y son fuente productora de hechos jurídicos ya que las transacciones financieras se configuran en código y quedan en la *Blockchain*, dejando la posibilidad de ser convertida a forma escrita para llevar a cabo acciones legales tal como lo establece la ley.

Por otro lado, tenemos el caso de Reino Unido, cuyo modelo ha sido precursor en la materia y seguido por muchos otros países. En el caso del Reino Unido no cuenta con regulación con fuerza legal vinculante, pero existe una declaración

jurídica del 2019 realizada por la *UK Jurisdiction Taskforce*, compuesta por expertos y con apoyo gubernamental. En ella, la *UKJT* abordó la naturaleza jurídica de los *Smart Contracts* y los consideró contratos con efectos legales siempre que cumplan los requisitos legales para considerar que de este surge una relación jurídica obligatoria entre las partes. Ésta declaración proporciona gran confianza en que los criptoactivos y en los *Smart Contracts* tiene una base sólida en la ley inglesa. Tomando como base que los contratos inteligentes reconocidos como acuerdos ejecutables bajo las leyes locales, la Comisión de Derecho del Reino Unido, afirmó que "no necesitan una reforma del derecho estatutario para los contratos legales inteligentes en el espacio de los activos digitales. (...) los contratos inteligentes construidos con tecnología de libro mayor distribuido son permisibles dentro del marco legal actual de Inglaterra y Gales. La Comisión de Derecho recomendó únicamente "un desarrollo incremental del derecho común", tal y como se necesita para los marcos existentes, pero también animó a las partes de los contratos inteligentes a explicar los riesgos relacionados con "la ejecución del código" y cualquier otro término necesario."

Otro país que se debe destacar es Italia en donde no se encontraba definido legalmente los contratos inteligentes, pero si poseía diversas normas relacionadas con el intercambio de criptoactivos y las *ICOs*, así como indicaciones de la Agencia Tributaria Italiana sobre la fiscalidad de la tenencia de criptodivisas. Sin embargo, la ausencia de normativa sobre los contratos inteligentes que hacían posible loas operaciones mencionadas, daba lugar a una grave falta de seguridad jurídica. Ello fue resuelto mediante el Decreto *Semplificazioni*, en donde se incorpora al texto legal las definiciones de *Blockchain* y *Smart Contracts*. Se define éste último como: "un programa informativo que opera mediante tecnologías de registro distribuido y cuya ejecución vincula automáticamente a dos o más partes sobre la base de efectos predefinidos. Asimismo, se considera que los contratos inteligentes no satisfacen el requisito de la forma escrita hasta tanto se produce la identificación informática de los interesados". De esta manera se incorpora el lenguaje código utilizado en los *Smart Contracts* como una nueva manera de concertar acuerdos entre las partes.

Por último, en relación a la regulación de *Smart Contracts*, se encuentra Estonia, que es un país que constantemente ha estado interesado a la innovación y acogimiento de nuevas tecnologías, de hecho, comenzó a incursionar en el mundo *Blockchain* en el año 2008. En 2012 fue el primer país del mundo en incursionar la tecnología de bloques, utilizándola como registro de datos gubernamentales. Por lo que no es extraño que en la actualidad, la adopción de ésta tecnología y la utilización de *Smart Contracts* sea una realidad aquí. En su legislación se establece que una firma electrónica reconocida y cualificada tiene la misma consideración que cualquier firma manuscrita, timbre o sello físico, por lo que el Smart contract se convierte en un método más a disposición de los estonios para efectuar contratación inteligente con plena eficacia legal.

En cuanto a la Protección de datos personales el mayor foco se aprecia en el *General Data Protection Regulation (GDPR)*, no solo por su importancia en Europa sino también por sus repercusiones en nuestro país, pues Argentina al formar parte de la comunidad internacional, busca el camino a la armonización de normativa y estándares con la Unión Europea. Hay que destacar que la finalidad del *GDPR* es dar control a los ciudadanos y residentes sobre sus datos

personales y simplificar el entorno regulador de los negocios internacionales unificando la regulación dentro de la U.E., es decir datos centralizadas. Es por ello que siendo la *Blockchain* descentralizada por definición, al menos en materia de *blockchain* públicas, muchos autores han afirmado que consideran que hay una incompatibilidad total con el *GDPR*, ya que los datos encriptados siguen siendo datos personales según la Directiva. Sin embargo, ello no es uniforme. Michèle Fink explica ésta problemática afirmando que: "una de las funciones que ofrece la *Blockchain* es de mantenimiento de registros que desecha de la necesidad de la intermediación de terceros y de esta manera, se puede descentralizar la recopilación, el almacenamiento y el procesamiento de datos. Ésta manera de trabajar con los datos es muy diferente a la actual que por el contrario centraliza los datos en forma de "poder de plataforma". *Google, Amazon, Apple* y *Facebook* son gigantes intermediarios quienes controlan cómo los individuos buscamos, compramos y nos conectamos. Así, recopilan, almacenan, procesan y monetizan de forma autónoma nuestros rastros de datos. Ello le permite aumentar su posición de poder utilizando dichos datos recopilados en su beneficio, con nuevos algoritmos por ejemplo. Tal poder de mercado ha causado preocupación desde la perspectiva de la política de competencia, ya que dificulta la entrada al mercado (...) las cadenas de bloques ofrecen la promesa del manejo descentralizado de datos y la soberanía de los datos, un concepto que se enfoca en dar a las personas el control sobre sus datos personales y permitirles compartir dicha información solo con partes confiables. El *GDPR* comparte el objetivo de la soberanía de los datos, ya que pretende otorgar a las personas físicas "control sobre sus propios datos personales".

Unos de los temas en el que colisiona el *GDPR* y los *Smart Contracts* es la determinación de actores intervinientes para el otorgamiento de obligaciones y/o derechos ya que. Ésto resultaría contrario a la esencia de la *Blockchain* en donde cada interviniente se sitúa en un plano de igualad siendo dificultoso determinar la condición de responsable y encargado de tratamiento de datos. Se ha recomendado la utilización de una red privada para que sea posible la adecuación a la normativa de la *GDPR*. Ante este entorno, es aconsejable operar en una red *Blockchain* privada, ya que los propietarios de la misma deciden quienes participa, siendo más sencillo la identificaron del rol.

Otro inconveniente es el suscitado por el derecho de supresión y el de rectificación, ya que se opera dentro de una red que es, en principio, por naturaleza inmutable. La *GDPR* establece que el interesado pueda solicitar intervención humana cuando una decisión automatizada produzca efectos jurídicos. Ello es contrario a la naturaleza de los Smart Contracts ya que funciona de manera automatizada sin intervención humana.

Más allá de las distintas problemáticas que se suscitan entre la *GDPR* y los *Smart Contracts*, lo cierto es que las distintas autoridades de protección de datos y diversos grupos de trabajo especializados, están en la búsqueda de la conciliación de ambas.

7. Marco Jurisprudencial

En el marco jurisprudencial no se ha podido encontrar casuística nacional o internacional en relación a la problemática como si lo hay respecto a la protección

de datos personales. Tanto nacional como internacionalmente la jurisprudencia es armoniosa en otorgarle protección al afectado.

Ésta autora estima que la falta de jurisprudencia es concordante con el nuevo paradigma. Para comprender, hay que tener en mente que todavía no se ha modificado nuestra ley de protección de datos personales en primer lugar, y en segundo, a nivel mundial, todavía se está discutiendo doctrinariamente la naturaleza jurídica de los *Smart Contracts* y hasta su definición.

8. Comprobación de Hipótesis

Luego de considerar los puntos más importantes relacionados con la protección de datos personales y su relación con los *Smart Contracts*, se puede concluir que el uso de contratos inteligentes en nuestro país provocará distintos escenarios, a saber:

En relación con la privacidad, dependerá de la cadena de bloques que se utilice– públicas o privadas– la forma de implementar las medidas de resguardo de los datos personales, en atención a la inmutabilidad existente en la red, ya que como detallamos, mediante los *Smart Contracts* se podría tener acceso a datos que pueden ser considerados personales para nuestra ley, como el caso de las llaves públicas, y en algunos casos, incluso podrían ser considerados datos sensibles.

Ya que Argentina forma parte de la comunidad europea y busca cumplimentar con los lineamientos de alta protección de datos personales, nos encontraríamos con las discusiones en relación al carácter inmutable de la *Blockchain*.

Ésta autora entiende que la utilización en sí de la *Blockchain* norepresenta un incumplimiento de la normativa de protección de datos. El mayor problema surge en el modo en el que se configure y utilice la tecnología lo que sí podría dar lugar a incumplimientos. Sin embargo, estos incumplimientos normativos que ocurren se deben a que la ley fue pensada para un escenario tecnológico diferente.

9. Propuesta

Una de las soluciones que se han propuesto en torno a la privacidad que se entiende que entra en peligro con la *Blockchain* es utilizar el denominado *Zero-Knowledge Proof. ZKP*. Éste método criptográfico refuerza la seguridad, privacidad y anonimato de la blockchain. Una de las premisas más innovadoras y atractiva de la cadena de bloques era la de proponer un lugar más seguro y privado para sus usuarios. Si a ello le sumamos un método de autenticación seguro como *ZKP, Blockchain* se encuentra con una alternativa a la privacidad mucho mayor a la que ya posee. Con Z*ero Knowledge Proof* tanto *blockchain* como sus servicios se encuentran con métodos de autenticación sin necesidad de revelar información sensible. Uno de los productos más famosos dentro de la criptografía es este nuevo protocolo. Después de todo, la seguridad, el anonimato y la privacidad se pueden conseguir con la combinación de estas características en la industria del *blockchain*.

Ésta autora entiende que utilizar *ZKP* en *Blockchain* sería una herramienta fundamental para contrarrestar la problemática en relación a la privacidad establecida en éste trabajo.

Por otro lado, en relación a la inmutabilidad y derecho al olvido la solución ya no se vislumbra tan simplemente. Luego del análisis realizado en el presente, ésta autora cree, sin eliminar la posibilidad de alguna solución técnica que desconoce, en pos del desarrollo tecnológico y los beneficios que encontramos dentro de la cadena de bloques y lo que se desprende de ello, serán los legisladores quienes deberán adecuar la regulación en materia de protección de datos personales teniendo en cuenta ésta característica de inmutabilidad y encontrar una alternativa para la protección de los datos personales y sensibles.

10. Conclusión y reflexiones finales

Para concluir, se afirma que la revolución en la era digital es innegable y que los nuevos paradigmas generan un panorama alentador para la sociedad y el mercado ya que simplifica procesos y elimina gastos. Si bien existen vacíos legales y contradicciones entre la naturaleza de la cadena de bloques y el ordenamiento jurídico, no por ello hay que quedarse en el tiempo.

Hay que ser conscientes de que el derecho debe acompañar a las nuevas realidades, regulándolas de la manera más justa. Por ello muchos juristas han afirmado que el derecho es una construcción social y así, necesitamos comprender las nuevas realidades y encontrar nuevas soluciones.

En este caso se necesitará del trabajo integrativo entre expertos en distintas ramas para darle un enfoque legal correcto al nuevo paradigma y poder integrarlo a nuestro ordenamiento jurídico y emplearlo como un conjunto más de herramientas digitales que permitirán acelerar y simplificar procesos, beneficiar el desarrollo y establecer mayor seguridad y transparencia web.

Bibliografía

https://abogados.com.ar/acercandonos-a-los-smart-contracts/28306 Última consulta 27/06/2022

https://www.austral.edu.ar/derecho/2019/04/01/adopcion-de-tecnologias-disruptivas-en-la-contratacion-publica-blockchain-como-herramienta-de-eficiencia-transparencia-y-aliado-contra-la-corrupcion/ Última consulta 27/06/2022

https://blogs.iadb.org/conocimiento-abierto/es/elementos-clave-de-blockchain/Última consulta 27/06/2022

https://core.ac.uk/download/pdf/288502094.pdf Última consulta 27/06/2022

https://earchivo.uc3m.es/bitstream/handle/10016/30195/TFG_Alvaro_Santos_Garcia_2019.pdf?sequence=1&isAllowed=y Última consulta 27/06/2022

https://earchivo.uc3m.es/bitstream/handle/10016/29653/TFG_Jose_Romero_Solis.pdf?sequence=1 Última consulta 27/06/2022

https://www.economistjurist.es/premium/derecho-inteligente/conflicto-entre-la-tecnologia-blockchain-y-la-normativa-de-proteccion-de-datos/ Última consulta 27/06/2022

https://edpl.lexxion.eu/article/edpl/2018/1/6 Última consulta 27/06/2022

https://es.cointelegraph.com/news/uk-law-commission-affirms-english-and-welsh-laws-apply-to-smart-contracts Última consulta 27/06/2022

https://es.crypto-economy.com/zero-knowledge-proof-zkp-que-es-y-como-funciona/ Última consulta 27/06/2022

https://www.fuerzas-armadas.mil.ar/Instituto-Ciberdefensa-FFAA/archivos/06%20FALIERO%20La%20proteccion%20datos%20personales.pdf Última consulta 27/06/2022

Gianfelici, F. (2020) "Smart contracts. ¿Crónica de un cumplimiento anunciado?" Argentina. La Ley 07/01/2019, 07/01/2019, 1 - La ley 2020-A, 547.

https://ir.lawnet.fordham.edu/jcfl/vol24/iss2/3/ Última consulta 27/06/2022

https://lawandbitcoin.com/regulacion-blockchain-2020-estonia/ Última consulta 27/06/2022

https://www.legalarmy.net/la-proteccion-de-datos-en-la-blockchain-y-los-smart-contracts-es-posible/ Última consulta 27/06/2022

https://legis.delaware.gov/json/BillDetail/GenerateHtmlDocument?legislationId=25730&legislationTypeId=1&docTypeId=2&legislationName=SB69 Última consulta 27/06/2022

https://legiscan.com/AZ/text/HB2417/id/1497439/Arizona-2017-HB2417-Introduced.html Última consulta 27/06/2022

https://legislature.vermont.gov/Documents/2018/Docs/ACTS/ACT205/ACT205%20As%20Enacted.pdf Última consulta 27/06/2022

Ley 27.275, articulo 19, Ley 27.483, articulo 1 y Ley 253326 articulo 2.

https://www.loyra.com/blockchain-y-normativa-de-proteccion-de-datos-una-relacion-tensa/ Última consulta 27/06/2022

https://revistaselectronicas.ujaen.es/public/journalslia/rej2021_21/151568764003/index.html Última consulta 27/06/2022

Mora, S. J. (2019) "La tecnología blockchain. Contratos inteligentes, ofertas iniciales de monedas y demás casos de uso" Argentina. La ley 01/04/2019, 01/04/2019, 1 - laley2019-B, 786.

Negri, N. J. (2022) "Smart Contracts". Publicado en: EBOOK-TR 2022 (Errico), 04/03/2022, 166.

http://openaccess.uoc.edu/webapps/o2/bitstream/10609/108706/6/atorrentiTFM0120memoria.pdf Última consulta 27/06/2022

Poncibo, C. (2022) "Smart contracts: moldeando los patrones futuros del consumo." Publicado: EBOOK-TR 2022 (Errico), 04/03/2022, 320.

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3875645 Última consulta 27/06/2022

https://periscopiofiscalylegal.pwc.es/blockchain-aplicacion-de-la-tecnologia-en-proteccion-de-datos/ Ultima consulta 27/06/2022.

https://repositorio.comillas.edu/rest/bitstreams/408683/retrieve Última consulta 27/06/2022

Notas de autor

* María Emiliana Flores es abogada egresada UNL 2015, cursando la especialidad en Derecho de la Empresa de la Universidad Nacional del Litoral. Tesis aprobada con distinguido en el curso independiente de posgrado Criptomonedas y Economía Digital. Smart Contracts y Blockchain de la Universidad Nacional de Buenos Aires en 2022.