

Derecho y Tecnología

EL SUPLEMENTO LEGAL DE NEURONA BA

MARZO 2021
ED: Nº03



Con el objetivo de acompañar el debate acerca de la expansión en el uso de las tic y su impacto en el derecho, desde Neurona BA lanzamos este suplemento sobre "DERECHO Y TECNOLOGÍA".

Tiene la coordinación de nuestro columnista habitual, el abogado, docente e investigador, Ernesto Liceda, con una amplia trayectoria en estas temáticas.

AUTORES

ERNESTO LICEDA // Coordinador del suplemento legal Tecnología y Derecho de Neurona BA.

CARLOS REUSSER MONSÁLVEZ // Abogado. Doctorado en Derecho, Universidad de Salamanca. Magíster en Derecho Constitucional, Pontificia Universidad Católica de Chile. Profesor de Derecho de la Información, Universidad Alberto Hurtado.

RODRIGO IGLESIAS // Abogado. Miembro del Observatorio de Derecho Informático Argentino.

FLORENCIA ROMINA GIANFELICI // Abogada. egresada de la Facultad de Ciencias Jurídicas y Sociales, Universidad Nacional del Litoral (UNL).

FERNANDO O. BRANCIFORTE // Abogado. Diplomado en Criptoconomía: Blockchain, Smart Contract y Criptomonedas (ITBA); y en Blockchain aplicable a negocios y relaciones jurídicas (UCC).

Recibimos comentarios y sugerencias vía mail a: neurona.buenosaires@gmail.com

PRÓLOGO

Por Ernesto Liceda



En este primer suplemento de Derecho y Tecnología de 2021 nos tomamos el atrevimiento de cumplir con el viejo dicho de que lo urgente no tape lo importante. Por ello el lector no va a encontrar artículos que hagan referencia a la pandemia que nos viene azotando desde el año pasado (aunque ya parece una década), no porque se desconozcan sus efectos directos en la relación derecho y tecnología, sino porque es necesario (y saludable) pensar en otras cuestiones.

Resulta imprescindible no olvidarnos de las muchas problemáticas que, derivadas de la relación derecho y tecnología, deben continuar siendo analizadas. Por ello en este suplemento encontraremos cuatro artículos de particular interés, tanto por la calidad de los trabajos como por el reconocimiento que cada uno de los autores tiene en sus respectivos campos. Como en otras ocasiones contamos con la participación de autores internacionales y nacionales de distintas provincias, que lo enriquecen particularmente.

En este número tengo la esperanza de que el lector, además de disfrutar y de encontrar utilidad a los distintos trabajos, sienta la imperiosa necesidad de ir a desempolvar los libros “clásicos” para poder entender mejor el Derecho Informático y la sociedad en la que vivimos.

En primer lugar tenemos el trabajo “¿Conoces a Argos Panoptes? Con seguridad, él te conoce a ti” del maestro chileno **Carlos Reusser Monsálvez**. Este trabajo, que parte desde la mitología griega, trata sobre un tema central en el mundo que nos toca vivir, el de la vigilancia masiva y permanente. Para muchos parecerá increíble que pueda hablarse con tanta solvencia del derecho informático partiendo de un ser mitológico con bastante más de mil años de antigüedad, pero puedo garantizarles que su lectura no sólo servirá para poner en cuestión muchos de los problemas actuales sino que, servirá de disparador para muchas formas de reinterpretar algunos temas.

A continuación, y muy vinculado al anterior, tenemos el trabajo del **Dr. Rodrigo Iglesias** “Sistema de

Identificación de Prófugos bajo la Lente del Derecho Informático” donde realiza un pormenorizado análisis del sistema de control biométrico del Estado sobre la ciudadanía, en base a un caso concreto en la Ciudad Autónoma de Buenos Aires. Este artículo nos permite poner en eje una discusión que data de hace ya cientos de años: hasta dónde puede la ciudadanía ceder libertad para aspirar a una incierta seguridad. Como siempre que leo sobre la dicotomía seguridad/libertad viene a mi memoria la frase de Benjamin Franklin “Quien renuncia a su libertad por seguridad, no merece ni libertad ni seguridad” y me tomo el atrevimiento de preguntar ¿hay seguridad sin libertad? Un reconocido jurista de mi querida Facultad de Ciencias Jurídicas y Sociales y miembro de la SCBA, el Dr. Hector Negri, solía decir en sus clases de Filosofía del Derecho que los derechos de uno no terminan donde comienzan los del otro sino que los derechos de uno comienzan donde empiezan los del otro. Tengo para mí que algo similar ocurre con la libertad.

Presentamos luego el trabajo ***“Nuevas Formas de Participación Democrática. PARTICIPACIÓN 2.0”*** de la ***Abog. Florencia Romina Gianfelici*** quien nos trae, desde la provincia de Santa Fe un interesante análisis de la participación de la ciudadanía por medio de las TIC. Sobre los distintos sistemas democráticos se ha hablado mucho y desde distintas perspectivas. Desde la idea romántica de la democracia griega hasta las virtudes y defectos de las democracias actuales hemos recorrido un largo trecho. Lo cierto es que por primera vez la tecnología permitiría, teóricamente, la participación de todos los ciudadanos en todas las decisiones. Esto me trae a la memoria lo escrito por Norberto Bobbio en su libro “El futuro de la Democracia” (ed. Fondo de Cultura

Económica 3° edición pág. 33) “El precio que se debe pagar por el compromiso de pocos es frecuentemente la indiferencia de muchos. Nada es más peligroso para la democracia que el exceso de democracia”. Como puede verse, un tema sumamente complejo e interesante.

Como colofón tenemos el artículo ***“Moneda digital Vs Moneda Virtual Vs Token Vs Criptomonedas Vs Dinero Electrónico ¿Todas caras de una misma moneda?”*** del ***Abog. Fernando O. Branciforte*** quien cuenta con una amplia trayectoria en el tema objeto del trabajo. En este artículo en particular podemos encontrar una muy clara explicación de las similitudes y diferencias que existen en este gran y complejo universo de las monedas digitales.

Demás está decir que lo relativo al control y la emisión de dinero “tradicional” ha ocupado vastas bibliotecas a lo largo de la historia, particularmente en lo que respecta a la intervención del Estado. Pero no puedo dejar de recordar aquellos “certificados” que otorgaban los templarios para el movimiento de bienes entre el territorio europeo y en tierra santa.

Que disfruten la edición, y que sea un espacio propicio para promover la reflexión y el debate.

¿Conoces a Argos Panoptes? Con seguridad, él te conoce a ti

Carlos Reusser Monsálvez

Doctorado en Derecho, Universidad de Salamanca. Magíster en Derecho Constitucional, Pontificia Universidad Católica de Chile. Profesor de Derecho de la Información, Universidad Alberto Hurtado

Si rebuscan en su memoria, tal vez encuentren el mito del gigante Argos Panoptes, quien tenía mil ojos, algunos de los cuales mantenía abiertos aun cuando estaba dormido.

Los trabajos que le encomendaban tenían que ver con ese talento; el último de ellos se lo asignó la diosa Hera: vigilar a la ninfa Io, amante de Zeus transformada en una ternera blanca, de forma que nadie se le acercara y que jamás escapara de su control.

Esos mil ojos y ese rol de Panoptes inspiraron a Jeremy Bentham en el siglo XVIII para proponer la creación del panóptico, una cárcel circular en cuyo centro hay un guardia que vigila a los presidiarios, pero su real poder es que estos nunca saben en qué momento concreto les están mirando y cuándo no, condicionando de esta forma su comportamiento al pesar sobre ellos la invisible omnisciencia de los vigilantes.

Más tarde Michel Foucault volvió sobre esta idea teorizando sobre si el diseño propuesto por Bentham era en realidad un poder que se ejercía no solo sobre los presidiarios, sino sobre toda la sociedad, plasmando sus postulados en el célebre libro “Vigilar y Castigar. Nacimiento de la prisión”, publicado en 1975.

Por supuesto, en la historia de la humanidad hay otras miles de ideas que han sido revisadas a lo largo del tiempo, sin necesidad siquiera de que haya pasado mucho tiempo desde su formulación.

Y una de ellas es el concepto de perfiles de personas, que durante mucho tiempo se entendió como la ordenación de determinadas características y cualidades humanas en aras de, posteriormente, determinar qué personas se encuadraban o encasillaban bajo qué perfiles.

Es decir, se definen unas pocas características que interesan y luego, dentro de un universo de muchas personas, se determina cuáles de ellas coinciden con el perfil.

Pero el desarrollo de las tecnologías de la vigilancia ha cambiado radicalmente la idea de lo que son los perfiles y, si somos sinceros, debemos admitir que los perfiles hoy en día en realidad son personas naturales, y esas personas han sido categorizadas en función de sus características, las cuales son conocidas gracias al tratamiento automatizado de sus datos personales que posibilitan determinar cuestiones específicas como su rendimiento profesional, situación económica, salud, preferencias sexuales, ubicación, intereses y un larguísimo etcétera.

Entonces, hay tantos perfiles como personas o, mejor dicho, cada perfil es exactamente una persona identificada o identificable: incluso el perfilado tiene un nombre que podemos conocer, si así lo deseamos.

Pero volvamos a nuestro gigante Panoptes o más bien a las tecnologías que permitieron, primero, vigilar a las personas en forma directa (como en el panóptico), y que luego posibilitaron llevar un

registro acabado de lo que las personas hacían en su día a día: el gigante puede ver no solo lo que las personas hacen en este momento, sino también lo que hicieron el pasado.

Y claro, si sumamos a lo anterior las posibilidades que brinda el procesamiento en línea de los datos personales a través del big data y técnicas de Inteligencia Artificial, Panoptes también puede ver el futuro del comportamiento de las personas.

Y no de las personas en general, sino que de cada persona concreta inserta en la Sociedad Red.

Es oportuno recordarles aquí, porque tiene consecuencias, que la Sociedad de la Información ya no existe, pues fue incapaz de cumplir sus promesas: las “tecnologías para la libertad” que propugnaba, que expandirían las libertades públicas, ensancharían los derechos de las personas y derribarían los prejuicios y las limitaciones al conocimiento, a partir del derribo de las torres gemelas en New York soportaron un duro vía crucis que las alteró en su esencia.

Y en la disyuntiva de morir, optó por transformarse, emergiendo en su lugar la Sociedad Red, esto es, todo un modelo social (diferente a lo previsto) que se levanta sobre una infraestructura de redes de comunicaciones electrónicas abiertas a las personas las que, a su vez, ejercen su ciudadanía y conforman sus redes humanas a través de plataformas sociales de base informática, interdependientes e interrelacionadas.

Es decir, que se ha modificado la forma en que tradicionalmente nos relacionamos con nuestro entorno y ahora lo hacemos a través de flujos de datos personales, que emitimos y recibimos constantemente; por eso, si no eres capaz de recibir y emitir datos a través de las redes de comunicaciones electrónicas, no eres parte de la sociedad, y no tendrás acceso a la información y las oportunidades que el resto sí.

Y en esa intermediación de datos, en el medio, vigilando el pasado, presente y futuro de cada persona está, con los mil ojos que nunca termina de cerrar, nuestro viejo conocido, Argos Panoptes.

No creo equivocarme al afirmar que, dentro de un sistema democrático, nunca nadie reunió tanto poder sobre los demás, pues ya no se limita a vigilar, sino que toma decisiones, y como los procesos de análisis de datos ocurren sin que las personas tengan conocimiento de ello, tampoco son conscientes de que en su vida diaria se están tomando decisiones que las afectan, derivadas de la observación y del tratamiento del detallado volumen de datos que contiene su perfil.

Y las decisiones que toma Argos Panoptes, según se ha venido demostrando, son cada día más automatizadas, superando las salvaguardias positivizadas en diversos instrumentos internacionales y leyes locales que afirman que es lesivo para la dignidad humana que una máquina tome decisiones o juzgue las personas.

Ejemplos clásicos de lo que ya está ocurriendo son los sistemas de evaluación de créditos, sobre todo en Norteamérica, en que las decisiones de las máquinas son finales y absolutas, aun cuando puedas explicar o justificar razonablemente la circunstancia que las máquinas señalan como fundamento para dejarte fuera del sistema crediticio.

Por supuesto que existen salvaguardias legales tanto contra la vigilancia masiva automatizada (que en el fondo es de lo que estamos hablando), como también contra las decisiones automatizadas respecto de las personas, pero sabemos que ambas cosas igualmente ocurren en el día a día; sin embargo nunca he sido partidario del realismo cínico que postula que “dado que no hay nada que hacer, no hagamos nada”.

Lo que sabemos con certeza es que Panoptes está presente no solo en las empresas transnacionales de servicios de Internet que todos utilizamos, sino también en nuestros propios Estados nacionales, particularmente en las compañías aseguradoras, consorcios comerciales, policías, agencias de inteligencia, entidades económicas y encargados de ciberseguridad del ámbito público y privado.

De hecho, todos estos entes comparten un objetivo en común: la eliminación de todo riesgo, y eso

garantiza su presencia, evidente u oculta, en los lobbies de los parlamentos nacionales ya sea abogando por la seguridad de las transacciones y el progreso de la economía digital, o pontificando sobre la seguridad del Estado y la protección de la infraestructura crítica.

Pero dejando lo anterior de lado considero en este momento más relevante abordar el tema de la relativa despreocupación del Reglamento General de Protección de Datos de la Unión Europea (devenido en estándar internacional), sobre el tema del perfilamiento y el uso de los mismos asociados a tecnologías de big data.

Admito desde ya que mi apreciación es algo injusta, pues lo del Reglamento no es realmente una despreocupación. De hecho, tanto en las disposiciones normativas como los Considerandos el Reglamento vuelve una y otra vez sobre los alcances de las tecnologías que permiten anticipar el futuro en base al tratamiento de los perfiles de las personas.

El problema es que, conociendo el poderío de Argos Panoptes, el Reglamento se reduce a establecer límites para el caso concreto, lo que se traduce en que la vigilancia masiva automatizada no es ilícita en la medida que se obtenga el consentimiento de los titulares de datos.

Y las tecnologías de la información tienen muchos mecanismos para obtener dicho consentimiento, partiendo por aquellas pantallas llenas de disposiciones contractuales que no leemos, pero respecto de las cuales no tenemos objeción en presionar el botón “Aceptar”, y que son aprovechadas por entidades de inteligencia para insertar cláusulas disimuladas que, en una muy libre interpretación, le dan acceso a los datos personales.

Aunque el problema de fondo es que nuestro sistema jurídico, en realidad, no tiene mucha relación con el Derecho Romano, contrariamente a lo que se nos ha dicho tantas veces, sino que con el sistema jurídico y económico de la revolución francesa, creado para cubrir los requerimientos de la triunfante burguesía y donde el “consentimiento” todo lo puede, aun cuando al persona sea inca-

paz de comprender los alcances de lo que ha aceptado; entonces, la normativa de protección de datos se ve constreñida a ese mismo marco.

Tratando de buscar un ejemplo para ilustrar el punto recordé el llamado Puente de los Suicidas (oficialmente, puente Villena) que se encuentra en la ciudad de Lima, el cual es conocido por ese nombre por obvias razones, y que las autoridades de Lima cubrieron para que la gente no se precipitara al vacío.

Pero en materia de protección de datos no hacemos lo mismo: como en el diseño jurídico el consentimiento de las personas todo lo puede, nos limitamos a exigirles que hayan expresado su consentimiento antes de lanzarse, lo que es con distancia uno de los talones de Aquiles de la normativa de protección de datos, y no veo que a corto o mediano plazo esté en el ideario de nadie cambiar esta situación.

También es digno de mención, en lo que se refiere a Reglamento de la Unión Europea y sobre todo por su influencia sobre las demás legislaciones, es que éste autoriza a Argos Panoptes a adoptar decisiones automatizadas sobre las personas en base a la predicción de experiencias, comportamientos y actividades, pero solo en la medida que “no les afecten significativamente”, concepto del todo abierto del cual habrá que ocuparse.

Pero hay un aspecto en el cual forzosamente los hombres de Derecho vamos a tener que meternos, como son los algoritmos de los sistemas de decisiones automatizadas, esto es el conjunto de secuencias e instrucciones que van asociados a las reglas que se aplican en las decisiones automatizadas pues, muchas veces en ellas, en forma invisible o casi inocente, van instrucciones incompatibles con un ordenamiento jurídico respetuoso de los derechos fundamentales de las personas.

Se los explico con el más cruel de los ejemplos que se ha presentado en Chile: en el año 2015 una niña de 13 años, llamada Daniela Vargas, tiene problemas con su corazón y requiere de un trasplante. Hay corazones disponibles, pero a ella se le niegan y se le envía a morir a su hogar y eso acontece.

Dos años después, cuando se le piden las explicaciones a la Red de Salud UC (entidad privada que gestionó el caso) sobre los fundamentos en que basaron la decisión, ellos dicen que aplicaron las reglas de negocio que usan siempre y una de ellas es que si quien va a recibir el órgano se encuentra en una “precaria situación social, familiar y personal” (es pobre), se le descarta como candidata por las bajas expectativas de sobrevida.

Es decir, por aplicación del “algoritmo”, la pobreza es un factor que te saca del listado de posibles beneficiarios de la donación de órganos.

Sabemos que Argos Panoptes es el nuevo dios supremo del panteón de la Sociedad Red, pero eso no quita que sea nuestro deber el revisar minuciosamente las reglas automatizadas que pretende aplicar y oponernos terminantemente aquellas que directa o indirectamente lesionen los derechos fundamentales.



Sistema de identificación de prófugos bajo la lente del derecho informático

Dr. Rodrigo Iglesias

Miembro del Observatorio de Derecho Informático Argentino

Como todos sabemos, los sistemas de identificación biométrica de personas se están implementando en varias ciudades del mundo y en pos de un bien jurídico que es tratado desde épocas de Hobbes, Locke y Rousseau el cual es evitar una muerte de forma violenta y realizando distintas concesiones para un Contrato Social, algunos problemas son ¿qué cedemos? ¿cuál va a ser su finalidad? ¿por cuánto tiempo? ¿y si quiero dejar de hacerlo?

Sabiendo esto, podemos decir que el 3 de abril de 2019 se realizó el “Primer Congreso Internacional de Delito Transnacional”¹ que se llevó a cabo en la Legislatura Porteña. En dicha oportunidad, el Ministro de Justicia y Seguridad de la Ciudad, el Sr. Mtro. Diego Santilli anunció la implementación de un nuevo sistema de reconocimiento facial (de ahora en más “SRFP” o “SRP”) que funcionaría también con “Inteligencia Artificial”. Donde entre otras cosas el Sr Ministro indicó que el sistema iba a estar funcionando en unas semanas generando conmoción en distintas organizaciones de la sociedad civil y en quienes entendemos un poco mejor como operan estos sistemas. El 29 de abril de 2019 se publicó la Resolución N.º 398/2019 en el Boletín Oficial de CABA donde se aplica de forma sorpresiva el Sistema de Identificación de Prófugos, sin una Ley emanada de la Legislatura, sino mediante una Resolución Ministerial, lo cual es un primer error y un detalle que nos deja un sabor amargo en cuanto al manejo de licitaciones dado que el mismo día del anuncio de la implementación del SRP a las 19:02hs fue publicado el Pliego de Bases y Con-

diciones Particulares para la Contratación Directa de un Servicio de el Análisis Integral de Vídeo (de aquí en adelante “el Pliego”) bajo PLIEG-2019 10400885 - GCBA – SSGA. Y tan solo 6 minutos más tarde ese pliego fue aprobado por las autoridades intervinientes publicando la Resolución 2019-59GCBA-SSGA. Este derrotero administrativo llevado en plazos poderosamente llamativos para los estándares usuales se vería finalizado pocos días después por medio de la suscripción de la Resolución 2019-98-GCBA-SSGA, de fecha 22 de abril de 2019, mediante la cual fuera aprobada la Contratación Directa N.º 2900-0472-CDI19. Finalmente, el flamante sistema comenzó a operar en la vía pública porteña el día 25 de abril de 2019.

Hasta aquí vemos algunas falencias en materia administrativa y técnicas que nos llaman poderosamente la atención, aún más cuando el propio Defensor del Pueblo formuló objeciones al sistema, pero fue una Organización de la Sociedad Civil que tomó el bastión, que consideramos correcto, efectuando un Pedido de Acceso a la Información Pública, conforme a la ley N.º 27.275. Dicho pedido obtuvo respuestas ambiguas o incompletas (la Administración no pudo responder de forma cierta gran cantidad de ellas) iniciándose un posterior amparo el cual el 6 de noviembre de 2019 la Justicia Contencioso Administrativo de CABA de primera instancia condenó al Gobierno de la Ciudad Autónoma de Buenos Aires a brindar la totalidad de la información solicitada por el Observatorio de Derecho Informático Argentino (en adelante ODIA), a la

fecha se encuentra a resolver por la Cámara de Apelaciones en lo Contencioso Administrativo por las distintas apelaciones presentadas por el Gobierno de la Ciudad De Buenos Aires.

El 22 de octubre de 2019, la legislatura de CABA sanciona la ley N.º 6.339 que modifica la ley N.º 5.688 en los artículos 478, 480, 480, 484, 490 y las incorporaciones de los artículos 480 bis y 490 bis, lógicamente la ley N.º 5.688 es la ley sobre el Sistema de Seguridad Pública y las modificaciones tienen que ver sobre la incorporación del Sistema de Identificación de Prófugos que el Ministro Santilli había implementado vía Resolución, para hacer caer en abstracto algunos de los planteos implementados por ODIA ante, por ejemplo, el análisis pormenorizado del Pliego. En dicha modificación se implementan 3 sistemas de “Identificación Biométrica” nombrados en el artículo 2 que modifica el artículo 480 de la Ley 5.688: “Sistema de Reconocimiento Facial de Prófugos, al Sistema Preventivo y al Sistema Forense” donde vemos un grosero problema al no contar con requisitos técnicos – legales para la implementación de cuáles y cómo deben operar esos tres sistemas.

Y es aquí donde empieza el problema legal y donde el Derecho Informático hace cuestión importante a la hora de implementar tecnología en la función pública, más aún cuando los derechos de la totalidad de los ciudadanos, nacionales o extranjeros, puede ser afectada, y aún mayor cuando un País vecino, como Uruguay, puede solicitar sanciones a nuestro País por no cumplir con Tratados Internacionales firmados por el País antes de la sanción de una Ley local.

En las distintas audiencias en el marco de la sanción de la ley, el Sr Profesor Joseph Cannataci dijo: “(...) Los ejemplos de otras ciudades han demostrado que la mejora de la seguridad pública mediante la instalación de cámaras de vigilancia es cuestionable en algunos casos y justificable en otros. La justificación de tal sistema, su legitimidad, necesidad y proporcionalidad deberían

haberse establecido mediante una evaluación del impacto en la privacidad (PIA, por su sigla en inglés) que no parece haberse llevado a cabo. **El hecho de que el reconocimiento facial se esté implementando sin el PIA necesario, así como la consulta deseable y las fuertes salvaguardias, también es motivo de preocupación. El Gobierno ha aprobado una reglamentación de bajo nivel en materia de biometría, pero no una legislación detallada sobre el uso del reconocimiento facial(...)**” cabe destacar, el Profesor Joseph Cannataci es el Relator Especial sobre Derecho a la Privacidad de las Naciones Unidas y sus dichos fueron sobre éste sistema de Reconocimiento de Prófugos². Ahora bien, ¿qué es un informe de impacto en la privacidad? Bueno, es un informe que se realiza de forma previa a la implementación de un sistema que puede vulnerar la privacidad, como lo hace dicho SRP al vulnerar Datos Personales Sensibles, desde la implementación del SRP por vía de Resolución del Ministro Santilli y aún siendo sancionada por la Legislatura de la Ciudad Autónoma de Buenos Aires el problema es de Derecho Internacional, dado que nuestro País firmó el denominado “Convenio 108”³ y es Miembro desde el 1 de junio de 2019, el Convenio 108 es el instrumento por el cual debemos tener un cuidado especial para el Tratamiento Automatizado de Datos Personales con Europa, pero también Uruguay lo firmó y debemos tener en cuenta que el principal acceso de uruguayos es vía marítima por el amaradero de Puerto Madero de una reconocida empresa.

A estos problemas locales, sumamos los diferentes fallos judiciales de otras Jurisdicciones, como en Estados Unidos, vemos que los sistemas de identificación biométrica como el SRP notamos distintos tipos de problemas legales en nuestro ordenamiento. El sistema tiene problemas de sesgos, como funciona con una base de datos (imágenes) y la carga no es “proporcional” ni mucho menos, da cuenta algo que en los resultados es tajante, las minorías siempre son perseguidas por errores de carga en esa base de datos,

entendamos que esas minorías son personas de, color, pobres, la comunidad LGTBQI+, pueblos originarios, partidarios de cierto color político, religiosos, etc. Ciertos Estados como Somerville, Massachusetts, San Francisco, Oakland prohibieron la utilización de tecnología de Identificación Biométrica por estos motivos.

Atento a las respuestas brindadas por el Gobierno de CABA sobre el pedido de Información Pública solicitado por ODIA es que podemos citar que el propio Ministerio brinda datos que nos dejan a la clara el mal desempeño y la falta de entrenamiento que tiene el sistema de identificación de prófugos o sistema de identificación biométrico cuando se nos plantea que al 30 de octubre de 2019 se habrían puesto a disposición de la justicia 1648 personas y sabemos que al 15 de agosto de 2019 las alertas arrojadas habrían sido 3059, podemos hacer una regla aritmética simple para determinar el estimado real de efectividad del sistema. Para ello, deberemos tomar la cantidad de personas puestas a disposición de la justicia (1648) y averiguar qué porcentaje representa del total de alertas arrojadas (3059). Para ello, una regla de tres simple será suficiente:

$1648/3059=0.538738*100=53.87\%$ de efectividad.

Como vemos es un sistema poco efectivo en la práctica y esos datos son brindados por la Administración con carácter de Declaración Jurada.

Nuestro País brinda esa base de datos mediante la CONARC, y esa base ya se encuentra errónea, pero por contener menores de edad entre los criminales buscados, con lo cual no se realizó un control adecuado y el SRP se alimentó de todos los menores que miraron a una de estas cámaras de reconocimiento facial, nuestro País ya fue denunciado por la ONG Human Rights Watch en fecha 9 de octubre de 2020 hemos recibido la noticia que la CONARC ha retirado la foto de un niño de 3 años de edad al cual se lo buscaba por ser prófugo de un “delito contra las personas – lesiones graves”.

Entendemos que esto se utiliza para que el propio sistema “aprenda” para pulir su algoritmo, pero ya tomó ribetes internacionales porque fue la ONG Human Rights Watch la que reportó el hecho. Finalmente la CONARC retiró de su base más de 17 personas menores de edad, pero, nuevamente, no sabemos como fue el borrado, si el Sistema de Reconocimiento de Prófugos mantiene esos datos biométricos para su identificación de parámetros y solo se retiró la obligación de emitir el alerta, si se sumaron datos de algún menor de edad que circuló por debajo de las 300 cámaras de ubicación rotativa que posee éste Sistema⁴. El problema es aún más grave dado que la ONG detectó 166 menores de edad en las bases de la CONARC. Si continuamos con la métrica es factible decir que casi 87 menores se encuentran siendo pasibles de una detención ilegal dado el porcentual de error del casi 52%.

El 23 de diciembre, el Observatorio de Derecho Informático Argentino inicia una Acción de Amparo en la Justicia Contencioso Administrativo de CABA solicitando que la Resolución N.º 398/MJYSGC/19, la Ley N.º 6.339 y sus modificaciones (la totalidad del SRP) sean suspendidas mediante una medida cautelar y dejadas sin efecto por no cumplir con el control convencional (el Convenio 108 mencionado) y el orden de afectación sobre la constitucionalidad de las normas como un sistema en conjunto, siguiendo las indicaciones de la Corte Suprema de Justicia en el Fallo Halabi “...En supuestos de conflictos colectivos que recaen sobre intereses individuales homogéneos” es por esto que el expediente se encuentra tramitando en segunda instancia en la Sala I de la Cámara de Apelaciones Contencioso Administrativa de CABA tras un rechazo de la controvertida Jueza Cabezas Cescato, donde no encontró un “caso”, dicha Jueza parece que olvidó la cantidad de detenciones por error que sufrieron una cantidad considerable de personas como Leandro Colombo Viña.⁵⁶⁷⁸

¹<https://www.casi.com.ar/1er-congreso-internacional-combate-del-delito-transnacional-y-los-procesos-de-integracion-3419/7>

² https://www.senado.gov.ar/bundles/senadomicrositios/pdf/observatorio_relator.pdf

³ <https://www.argentina.gov.ar/noticias/argentina-se-suma-al-convenio-108>

⁴ <https://elpais.com/internacional/2020-10-09/hrw-denuncia-que-argentina-publica-en-linea-informacion-de-menores-acusados-de-delitos.html>

⁵ https://tu.com.ar/policiales-de-un-dni-mal-cargado-una-cara-parcida-las-victimas-del-sistema-de-reconocimiento-facial-en-buenos_980528/

⁶ <https://www.presescader.com/argentina/clarin/20190723/281956019377677>

⁷ <https://www.pagina12.com.ar/213721-la-defensoria-del-pueblo-objeto-el-sistema-de-reconocimiento>

⁸ <https://www.unsam.edu.ar/tss/luz-camara-y-control/>

Nuevas formas de participación democrática. Participación 2.0

Florencia Romina Gianfelici

Abogada egresada de la Facultad de Ciencias Jurídicas y Sociales,
Universidad Nacional del Litoral (UNL)

"El espíritu democrático se basa en esta conciencia de la interdependencia entre la unidad y la diversidad..."

Continuará al final del trabajo.

Adaptación al cambio

En las últimas cuatro décadas se han evidenciado importantes debates doctrinarios en torno a la función del Estado. Así, de una administración pública tradicional de neto corte weberiano, caracterizada por la racionalidad y el estricto apego a la norma, el desarrollo de los estados de bienestar exigió desagregar, desde lo organizativo, las estructuras centralizadas del modelo antecesor.

En esta órbita el “ciudadano-usuario”, que hasta aquel entonces desempeñaba una actitud meramente reactiva frente a una burocracia rígida, pasó a posicionarse como un “ciudadano-cliente”. Es decir, un ciudadano con legitimidad para reclamar el cumplimiento de las políticas públicas en expansión como si fuesen objetivos propios de dinámicas empresariales.

Sin perjuicio de ello, tanto la administración pública tradicional como la nueva gestión pública, se centraron en lo que sucede dentro de sus estructuras, relegando a un segundo plano el papel del ciudadano en la toma de decisiones.

Frente a esto, se gesta un nuevo modelo de gobernanza, que bajo los postulados de transparencia, participación y colaboración se ha dado en llamar Gobierno Abierto (Open Government). Este

propone la configuración de nuevas administraciones públicas colaborativas, que salen al rescate de una ciudadanía involucrada. Se busca de esta manera la incorporación de conocimientos colectivos dispersos en la sociedad dentro de aquellas estructuras administrativas, que originariamente los excluían.

Participación como eje

La participación ciudadana se vio fuertemente transformada por el uso de Internet. Es precisamente, bajo la órbita de la filosofía 2.0, donde surgen nuevas formas de gestión de la información pública y su consecuente aplicación en la resolución de problemas sociales.

Este modelo de producción de información online peer-to-peer se ha dado a llamar Crowdsourcing. Consiste en un proceso de resolución de problemas (problem-solving), esto es una actividad participativa donde, en este caso la administración pública, propone a la colectividad (más o menos experta e implicada en la problemática que hay que tratar) la resolución voluntaria y conjunta de un problema. De esta manera la decisión pública no sólo tiene fundamento en una única voz experta, sino en el sentir de una colectividad, de un grupo de ciudadanos amateurs, donde todos

aportan algo.

En este sentido el usuario del servicio se convierte en productor activo del mismo generando una retroalimentación beneficiosa para organizaciones e individuos. La identificación de centros de interés, la disponibilidad de datos masivos, la existencia de plataformas sociales que sirvan de sensores y herramientas de escucha activa, resultan de vital importancia en esta tarea.

Imaginemos que el gobierno municipal tiene que autorizar la construcción de un edificio dentro de la ciudad y, como decisor, no cuenta con toda la información sobre la problemática en cuestión. Podría acudir a un pequeño comité de expertos en la materia, o recabar información de aquellos vecinos a los que aquella decisión afectaría directamente.

Ejemplos reales de la utilización de esta tecnología es el caso de Future of Melbourne 2026, plataforma colaborativa donde los ciudadanos participan de la planificación del futuro de la ciudad. Como igualmente, lo implementado en la provincia de Santa Fe: con motivo de la reforma constitucional se ha creado la plataforma digital “Bases para la Reforma” (www.basesparalareforma.digital), en donde los ciudadanos pueden aportar, de manera on line, sus pareceres al respecto. De tal modo se obtiene que la futura convención reformadora tenga la mayor legitimidad social posible. Las soluciones a las que arriben a través del mecanismo digital antedicho serán sumamente valiosas, desde que sus destinatarios han participado con diferentes visiones de la cuestión planteada, convirtiéndose así en coproductores de aquellas.

La Participación 2.0 como nueva forma de participación ciudadana

Ha quedado demostrado en los apartados precedentes que es sumamente importante contar con el ciudadano en la gestión de lo público, el tema es cómo.

La existencia de procedimientos formales de participación no la garantizan. De hecho, la excesiva burocratización ha gestado organismos de participación pesados en su convocatoria, mantenimiento y operatividad. Es más, una sumatoria excesiva de los mismos puede generar un desgaste técnico en la propia ciudadanía mermando todo tipo de dinámica social. No sólo se resienten los procesos sino la calidad de los mismos.

Lamentablemente la práctica nos ha demostrado que las expectativas, muy altas, de participación ciudadana, no fecundaron en la sociedad moderna postindustrial. La preocupación por lo público no es algo que el común de los ciudadanos ponga en el centro de sus vidas, algunos por desinterés y otros por la falta de convencimiento de que su opinión sea valorada.

Entonces cabría preguntarnos qué es lo queremos lograr. Claramente que no sólo propiciamos agilizar la participación ciudadana a partir de la simplificación de sus metodologías sino lograr una intervención de calidad. Debemos crear medios de escucha más novedosos y flexibles, que atraiga al ciudadano a colaborar en beneficio suyo y de su comunidad.

En estos cometidos, las Tecnologías de la Información permiten catalizar una nueva participación ciudadana. La e-participación, participación electrónica o participación 2.0, esto es a través de plataformas digitales, facilita la búsqueda, filtro y sistematización de aquella información valiosa en el manejo de lo “público”.

De más está decir que las redes sociales no son un procedimiento formal de participación ciudadana como los mecanismos de democracia semidirecta mencionados en los arts. 39 y 40 de nuestra Constitución Nacional, pero sin perjuicio de ello aquellas se han convertido en un canal ideal para incidir en las políticas públicas.

Ahora bien, la intervención en las redes sociales no debe leerse como una mera reproducción o

juxtaposición de lo que ocurre en las estructuras administrativas del mundo offline, sino que el verdadero desafío es poner en acción la capacidad creativa de la ciudadanía. Se busca así, que las redes sociales sean los nuevos espacios de interacción y de comunicación en la esfera pública.

Lo cierto es que las administraciones han adaptado la tecnología de manera lenta y desigual. A punto tal que, para aquellas acostumbradas a la rutina procedimental y reglamentaria, esta presencia “obligada” en el mundo digital, motivada por la situación de pandemia que estamos transitando, ha sido un verdadero salto al vacío, que desafía el ingenio de los administradores.

Ventajas y desventajas de estas modernas formas de participación

Como dijimos en los apartados precedentes, el hecho de que las políticas públicas sean expresión de las preferencias del ciudadano garantiza en mayor medida su cumplimiento. En este orden, la participación 2.0 reduce la posibilidad del fracaso en su implementación al poder anticiparse a las necesidades de la población. Ello a tenor que las decisiones que se adopten habrán sorteado el tamiz de la opinión pública.

Así, la contribución del ciudadano con nuevas ideas es un trampolín hacia la creación cooperativa de soluciones incrementando las posibilidades de satisfacción de las necesidades sociales. Las administraciones ceden su rol protagónico frente al ciudadano que pasa a ser un nodo más de un complejo entramado social.

Ahora bien, esta visión optimista del uso de las TICS en el ámbito de lo público no es compartida por todos. Una de las problemáticas que mencionan sus detractores son los mayores costes en la toma de decisiones. Toda decisión política requiere del consentimiento de un mayor número de actores con intereses y puntos de vista disímiles. Se sostiene entonces que la falta de canales aptos para integrar efectivamente estas demandas

en el seno de la estructura organizativa puede generar un efecto "boomerang" que tire por la borda las oportunidades que brindan estos nuevos medios de participación.

A esto le suman los problemas de inclusividad y participación derivados de las dificultades del aprendizaje que genera la brecha tecnológica, y las tensiones o disfunciones organizativas producto de una reducida o desbordada participación ciudadana.

Sin embargo, todas estas desventajas que se mencionan son comunes a otros modos participativos. Se trata de valladares superables con una correcta explicación del objetivo de su implementación y la capacitación de los agentes involucrados tanto administradores como administrados.

Conclusión

El descrédito general hacia la política convencional hace notar los límites de la democracia representativa y da cuenta que una dosis de democracia participativa está a la orden del día. Es cierto que la participación directa no puede pensarse como la solución a los problemas políticos de las sociedades actuales, pero los medios tradicionales de democracia semidirecta no han corrido mejor suerte.

Frente a esto, Internet y las redes sociales hacen surgir una nueva forma de participación que difiere de la tradicional, con nuevos retos y oportunidades.

Es de esperar que la proporción de la población involucrada sea la razonablemente interesada en los temas de que se traten. Que una cuestión pueda ser deliberada y debatida en un foro abierto, distinto al convencional, augura el éxito de su solución.

El camino recorrido hasta aquí es muy corto y en permanente construcción. El triunfo de estas aplicaciones tecnológicas depende en gran

medida de la capacidad del sector público para alterar las reglas de funcionamiento actuales y la concientización de una ciudadanía acerca de la bondad de tal posibilidad informática.

Como lo prometido es deuda, la frase del comienzo de nuestro trabajo así continúa:

"... y se nutre de un debate permanente sobre la frontera, constantemente móvil, que separa a una de otra, y sobre los mejores medios de reforzar su asociación."

Alain TOURAINE



Moneda digital Vs Moneda Virtual Vs Token Vs Criptomonedas Vs Dinero Electrónico

¿Todas caras de una misma moneda?

ABOG. FERNANDO O. BRANCIFORTE

Diplomado en Criptoconomía: Blockchain, Smart Contract y Criptomonedas (ITBA); y en Blockchain aplicable a negocios y relaciones jurídicas (UCC)

Introducción

A lo largo de la historia de la humanidad, la moneda ha sido el punto característico y el medio para adquirir bienes y para intentar conseguir esa “seguridad” y/o “libertad financiera” que busca el ser humano.

Pero, con el paso de los años, el bien utilizado para esos fines no es el mismo que existe hoy en día y, si bien esto parece un análisis de gran obviedad, nunca está de más tomar conciencia que, lo que hoy llamamos “moneda” o “dinero” no es lo mismo que aquello de antaño.

En este sentido, si lo que hoy nombramos como “moneda” o “dinero” no es igual a aquello referido por nuestros antepasados, muy probablemente lo que hoy no llamamos “moneda” o “dinero” si lo sea.

Ahora bien, con el trabalenguas del párrafo anterior lo que nos queda claro es que, al día de hoy no podemos definir concretamente las diferentes “clases” de moneda o dinero que existen.

E incluso, observe el lector, que estamos utilizando las palabras moneda y dinero como sinónimos cuando no lo son. Y esta confusión aumenta aún más hoy cuando con la tecnología aparecen otros medios de intercambio financiero que nos cuesta definir.

Es así que, en el presente artículo, nos proponemos traer un poco de luz a estos conceptos que tantas confusiones generan y que, en gran cantidad de ordenamientos jurídicos, son utilizados como sinónimo cuando, adelantamos, no lo son.

Dinero o moneda

En este sentido debemos comenzar a analizar cómo la moneda o dinero, como bien de cambio, hoy adquiere diferentes modalidades.

Si remontamos a la historia, y sin entrar en detalles, podemos ver que el trueque y los metales preciosos eran aquellos medios preciados de valor para adquirir bienes. Luego aparece la moneda como metal precioso acuñado para pasar al papel moneda o billete como indicador de valor.

Pero hoy en día, y más aún con el avance de la pandemia y de la tecnología, todo aquello pareciera ir desapareciendo hasta convertirse todo en 0 y 1, en códigos binarios, en pagos electrónicos a través de tarjetas de crédito, de débito, prepagas, códigos qr, transferencias bancarias, entre otras.

Es decir, si bien aquellos sistemas nombrados hoy siguen existiendo, en la actualidad es más común encontrar sistemas de pago informáticos y, en estos sistemas, es donde comienzan a aparecer distintos conceptos como dinero electrónico, moneda digital, moneda virtual, token o criptomoneda.

Y, justamente estos nuevos conceptos tan distintos y tan similares a la vez, generan gran confusión no sólo en los ciudadanos sino también en los legisladores quienes, a la hora de crear las normas, los utilizan muchas veces como sinónimos cuando no lo son.

Con lo cual, la pregunta que se hará el lector es, ¿Qué son? ¿En qué se diferencian? ¿Tienen alguna relación entre sí?

Dichas preguntas intentaremos responderlas en el punto siguiente desarrollando cada una de ellas de manera muy breve por la extensión del presente artículo.

Moneda digital Vs. Dinero Electrónico Vs. Moneda Virtual

Los conceptos de moneda digital, moneda virtual y dinero electrónico son aquellos que más dolores de cabeza traen en el mundo de las finanzas electrónicas.

Tal es así que, por ejemplo, la Ley 27.430 habla de moneda digital cuando pareciera que es otro el fin hacia donde apunta, mientras que por otro lado la CNV, el BCRA y la UIF hablan de monedas virtuales, y a su vez, todas parecieran referirse a las criptomonedas. Entonces ¿Son sinónimos? ¿Cómo poder ubicar los conceptos originarios para poder desmembrar a que nos referimos realmente?

Para ello es recomendable comenzar recurriendo a las indicaciones internacionales presentadas por GAFI en 2014, allí establece lo siguiente:

“Monedas digitales debe entenderse como una representación digital de cualquier moneda virtual (no dinero fiduciario) o de dinero electrónico (dinero fiduciario)”

Es decir, de la definición dada por GAFI, podemos observar que el término “moneda digital” hace alusión al género de toda representación digital en la cual incluye a los términos “moneda virtual” y “dinero electrónico”.

Asimismo, de dicha definición vemos la existencia de la diferencia entre moneda virtual y dinero electrónico en que este último es dinero fiduciario mientras que no lo es la moneda virtual.

En otras palabras, si comenzamos a armar un árbol vemos que tenemos como principal centro a la moneda digital y de allí se derivan dos ramas separadas y diferentes como son la moneda virtual y el dinero electrónico.

La definición así diferencia entre moneda virtual y dinero electrónico, también podemos encontrar lo mismo en la Resolución 300/14 de la UIF, la cual expresa que la moneda virtual es:

“...la representación digital de valor que puede ser objeto de comercio digital y cuyas funciones son la de constituir un medio de intercambio, y/o una unidad de cuenta, y/o una reserva de valor; pero que no tienen curso legal, ni se emiten, ni se encuentran garantizadas por ningún país o jurisdicción. En este sentido las monedas virtuales se diferencian del dinero electrónico, que es un mecanismo para transferir digitalmente monedas fiduciarias, es decir, mediante el cual se transfieren electrónicamente monedas que tienen curso legal en algún país o jurisdicción”

En este punto podemos diferenciar más concretamente la moneda virtual del dinero electrónico en que solamente este último tiene curso legal en algún país o jurisdicción y no así la moneda virtual.

En igual sentido, en 2015 GAFI reafirma esto al decir:

“las monedas virtuales se distinguen de las monedas fiduciarias (también conocidas como monedas reales, dinero real o moneda nacional), toda vez que las últimas se caracterizan por ser dinero moneda y papel de curso legal en un país, circulan y son habitualmente utilizadas y aceptadas como medio de cambio en su país de emisión”

Justamente, siguiendo con esta idea, debemos hacer referencia a que con moneda virtual, como especie de moneda digital, estamos hablando específicamente de aquellas “monedas” utiliza-

das en los distintos juegos virtuales.

Hoy en día existen juegos como Second Life, Diablo, World of Warcraft, entre tantos otros donde se crean mundos virtuales en los cuales existe su propia moneda que debemos utilizar para adquirir (comprar) ciertos beneficios o mejoras a nuestro personaje. Estas monedas son monedas virtuales por cuanto no tienen curso legal en ningún país pero, en algunos casos, se han convertido en unidad de valor.

Ahora bien, sabemos que la moneda digital es el género, sabemos que de la misma se deriva el dinero electrónico y la moneda virtual diferenciándose una de la otra respecto al curso legal o la emisión de un país pero, ¿en dónde entran las criptomonedas? ¿Y los tokens? ¿Son moneda virtual o dinero electrónico o una especie ajena?

Criptomonedas Vs. Tokens

Para poder encontrar una definición lo más cierta posible y ver si la criptomoneda y los tokens son iguales, son distintos, o si son moneda digital o si son moneda virtual debemos primero recurrir a un diccionario.

El diccionario de Oxford nos define a las criptomonedas como:

“Una moneda digital que emplea técnicas de cifrado para reglamentar la generación de unidades de moneda y verificar la transferencia de fondos, y que opera de forma independiente de un banco central”

Ya aquí notamos que forma parte del género moneda digital con la característica de contar con técnicas de cifrado y que es independiente de un banco central. Con lo cual, si bien es parte de una moneda digital se diferencia del dinero electrónico en que no deriva de ninguna entidad estatal.

Por otro lado, en el 2018, GAFI al referirse a las criptomonedas dice que son un activo virtual y

define activo virtual de la siguiente forma:

«Un activo virtual es una representación digital de valor que puede ser digitalmente comercializada/intercambiada o transferida, y que puede ser utilizada como medio de pago o de inversión. Los activos virtuales no incluyen representaciones digitales de monedas fiduciarias, valores negociables (securities) u otros activos financieros que se encuentren cubiertos en otros puntos de la Recomendaciones del GAFI»

Sin embargo, esta definición termina trayéndonos aún más dudas por cuanto nos agrega un nuevo concepto a la lista, el de activo virtual.

Nuestro país, para definir a las criptomonedas recurre a la UIF, la cual solamente ha desarrollado la definición nombrada de moneda virtual, es decir lo asimila a moneda virtual como sinónimos.

Lo cierto es que la criptomoneda, si bien puede considerarse una moneda virtual por cuanto es una representación digital de valor, es una unidad de intercambio, puede ser objeto de comercio digital y, en principio, no tienen curso legal, deben diferenciarse de las denominaciones brindadas en el punto anterior por cuanto toda criptomoneda tiene por detrás a la tecnología blockchain y a un sistema criptográfico que la respalda, a diferencia por ejemplo de las monedas virtuales de un videojuego.

Es en este sentido que consideramos que la criptomoneda es una moneda virtual pero con tecnología blockchain. Es decir, si volvemos al “árbol” inicial de este artículo, podemos encontrar a la moneda digital como género de la cual se deriva la moneda virtual y el dinero electrónico y, a su vez, de la moneda virtual se deriva como subrama o subclase a las criptomonedas cuando tienen detrás a la tecnología blockchain. Pero, ¿y los tokens?

Según William Mougayar en The Business

Blockchain, podemos definir a los Tokens como:

«Una unidad de valor que una organización crea para gobernar su modelo de negocios y dar más poder a sus usuarios para interactuar con sus productos, al tiempo que facilita la distribución y reparto de beneficios entre todos sus accionistas»

Así los tokens pueden servir para otorgar derechos, como equivalencia de valor monetario, para ceder datos, para ceder derechos, como pago por un trabajo, como puerta para servicios, para aquello que la organización o la persona que lo crea le dé valor o utilidad.

Una clasificación actual y aceptada divide a los tokens en tres clases:

Payment Token: se usa como medio de pago.

Utility Token: da derecho a servicios o funcionalidad.

Security Token: representa un activo, una deuda o una participación de futuros ingresos.

Conforme esta clasificación, un Payment token podría ser considerado moneda virtual, y a su vez, al tener tecnología Blockchain debería también ser considerado criptomoneda. Sin embargo, como existen otros tipos de token podemos afirmar que toda criptomoneda es un token pero no todo token es una criptomoneda.

Conclusión

Como conclusión del presente artículo podemos decir que los conceptos que muchas veces son utilizados como sinónimos en realidad son, en la mayoría de los casos, género y especie.

Así, como resumen final podemos armar el siguiente árbol: La moneda digital es el género del cual derivan la moneda virtual y el dinero electrónico diferenciándose en el hecho que éste

último tiene curso legal y es emitido por un estado; a su vez si a la moneda virtual se le aplica tecnología blockchain estamos frente a un token, el cual si tiene la función de ser un medio de pago o intercambio de valor podrá ser llamado criptomoneda.

Consideramos que, el hecho de entender y estudiar en profundidad los conceptos hará que las normas sean más claras y de mejor aplicación y muchas veces lo que parecen ser sinónimos no son más que una especie dentro del género y, el saber diferenciarlas (tanto por parte del regulador como del usuario) llevará a una seguridad jurídica necesaria en todo ámbito.

