#LEGALTECH II

El Derecho ante la Tecnología

SUPLEMENTO ESPECIAL

OCTUBRE 2019

Directores
GASTÓN E. BIELLI
SANTIAGO J. MORA
DIEGO FERNÁNDEZ

THOMSON REUTERS

SUPLEMENTO ESPECIAL

OCTUBRE 2019

#LEGAL**TECH II**

El Derecho ante la Tecnología

Directores:
GASTÓN E. BIELLI
SANTIAGO J. MORA
DIEGO FERNÁNDEZ

Bielli, Gastón Enrique
#Legal Tech II / Gastón Enrique Bielli; Santiago J. Mora; Diego Fernández. - 1a ed. - Ciudad Autónoma de Buenos Aires: La Ley, 2019.
160 p. ; 24 x 17 cm.

ISBN 978-987-03-3859-8

1. Derecho Informático. I. Mora, Santiago J. II. Fernández, Diego III. Título
CDD 346

Tucumán 1471, 1050 Buenos Aires
Queda hecho el depósito que previene la ley 11.723
Impreso en la Argentina

Tirada: 1400

ÍNDICE GENERAL

El evento Legal Tech Summit 2019 en clave con el mundo digital

MARÍA BELÉN ALVAREZ ECHAZÚ (*)

"Esto es solo el comienzo". Con esa frase, José Domínguez, Head of Legal Professional de Thomson Reuters, marcó la apertura del evento **"***LEGAL TECH SUMMIT:* Transformación digital de la profesión #SinPrecedentes**"**, que tuvo cita el miércoles 3 de julio, donde *techies* de primera línea expusieron, frente a una gran audiencia de abogadas y abogados, lo último sobre inteligencia artificial, *big data*, *machine learning*, *smart contracts*, *fintech*, *data privacy*, seguridad informática y los desafíos del expediente electrónico. Así, en una maratónica sesión de cinco paneles, Thomson Reuters fijó un punto de partida para el debate y marcó la agenda de los retos que depara la innovación tecnológica para el mundo legal. ¿Qué nos dejó el *Legal Tech*?

"Pensemos como era un estudio jurídico veinte años atrás y como se trabajaba, los problemas que había. Hoy todo eso cambió porque cambió el mundo, la forma de trabajar y de hacer cosas. Pensemos en las distintas tecnologías. Creo que todos escucharon hablar de *big data*, inteligencia artificial, *blockchain* y *smart contracts*. Si alguno no escuchó, por favor preocúpese", destacó Domínguez. En esa línea, remarcó la necesidad de ser curiosos y de mente abierta, al mismo tiempo que resaltó el rol de la diversidad y la inclusión de nuevos perfiles —*data science*, *legal design*, etc.— en los estudios jurídicos y departamentos legales.

En el primer panel "Procedimiento y Prueba Judicial Digital", se presentó el proceso electrónico de un lado y del otro del mostrador. Así, Gustavo Pérez Villar, prosecretario en la Subsecretaría de Tecnología Informática de la SCBA, expuso sobre el sistema bonaerense, los desafíos de la firma digital, la nueva versión del Portal de Notificaciones y Presentaciones Electrónicas y las innovaciones que van a venir gracias a "AUGUSTA".

Por su parte, Hernán Quadri, secretario de la Cámara de Apelación Civil y Comercial de Morón, subrayó la idea de que no se puede pensar al expediente electrónico con la lógica papel. "¿Cuál es la idea del expediente digital? ¿La idea es despapelizar nada más? Nos quedamos bastante cortos. Es inadecuado pensar el expediente digital como el expediente papel. El expediente digital implica repensarlo todo".

En esa línea, Raúl Farías, director Académico IT - PEA en FORES, propuso abandonar la idea de un expediente lineal y dar paso a la hipertextualidad, admitir todo tipo de archivo digital, permitir la composición de archivos digitales, tratar la información con IA y *machine learning* y aprovechar los resultados. "Tenemos que ir hacia un expediente inteligente", arriesgó.

En último lugar, Gastón Bielli, presidente del Instituto Argentino de Derecho Procesal In-

(*) Abogada de la Facultad de Derecho de la Universidad de Buenos Aires. Máster en Periodismo de la Universidad Torcuato Di Tella y La Nación.

formático, preguntó a los presentes: "¿Cómo se certifica que un contenido fue publicado online? ¿Con un print de pantalla? ¿Por escribano? ¿Y si a las dos horas no está más o es un fin de semana?". Así, el especialista asombró a la audiencia con una presentación disruptiva de los terceros de confianza (1).

El panel "*Smart Contracts* - Empresas *Fintech*" contó con la presencia de Hugo Acciarri, director del programa de "Derecho, Economía y Comportamiento" de la UNS y profesor de posgrado. "¿Qué tenemos que ver los abogados con los *smart contracts*?", preguntó. Con ese disparador, brindó precisiones terminológicas (¿qué es la inteligencia?) y habló de filosofía, IA, contratos parcialmente automatizados, criptomonedas y *blockchain* (2).

Incluso en ese contexto, Acciarri brindó un consejo que ningún estudiante y abogado debería dejar de escuchar (y tomar): "Las habilidades que tenemos para relacionarnos con los que saben más que nosotros de otras profesiones van a valer más que sabernos de memoria los artículos de la última ley. Un abogado que trabaje en este nuevo ecosistema deber ser un abogado abierto a utilizar sus escasos conocimientos para aportar valor a estas nuevas cosas. Mi propuesta es que aportemos valor. Tenemos mucho para hacer".

Luego, en el mismo panel, Santiago Mora, socio en GPG *Advisory Partners* y profesor "*Fintech Law*", trabajó sobre el concepto *fintech*, las cuestiones que hacen compleja su regulación y los negocios de pago. "¿Qué se entiende por *fintech*? Es una pregunta muy fácil pero la respuesta no. La palabra se usa de distintas maneras, no es una palabra clara en lo relativo a qué incluye y a qué excluye. Un poco porque es nueva y otro poco porque está de moda y se sobre utiliza", precisó.

Entonces, el especialista *fintech* resaltó que la Argentina está ante una oportunidad muy importante y, por lo tanto, "es un desafío más importante aún no arruinarla". "Tenemos el material y tenemos la necesidad. Lo que tengamos que hacer, ya sea que elijamos regular, no regular o autorregular, lo que sea que queramos hacer, lo tenemos que hacer de manera inteligente y debatida. Esto tiene que resolverse con todos: los reguladores, todas las empresas, las grandes, las chiquitas, las que tengan solo proyectos, la sociedad civil y la academia", aseveró.

En el tercer panel, llegó el turno del *trending topic* de la *data privacy* (claramente, el 2019 se puede destacar como un año plagado por multas millonarias a las gigantes tecnológicas por violaciones a la privacidad (3)), con foco en el uso de datos personales para el marketing y geolocalización de dispositivos móviles, con las presentaciones de Lisandro Frene, socio en Richards Cardinal Tutzer Zabala & Zaefferer a cargo del Departamento de IT, y Diego Fernández, Socio de Marval, O'Farrell & Mairal.

Frene señaló que, en el procesamiento de datos personales, surgen preguntas como: ¿es legal comprar una base de datos a una agencia de marketing? ¿Es legal ceder la base de datos de mis clientes a un tercero para que publicite sus bienes o servicios? ¿Es legal combinar datos de un banco, una prepaga y una aseguradora para *cross selling*? ¿Es legal captar datos de redes sociales y procesarlos para marketing?

Al respecto, afirmó: "En Argentina aparentemente es legal usar indiscriminadamente datos personales de las personas alegando fines publicitarios. Yo creo que es equivocado, que la ley argentina está mal pero la letra dura avala hacerlo. Lo más grave no es la oferta con spam o un llamado en medio de una reunión, sino lo que hay detrás para hacer ese llamado o dirigirles spam: una persona que conoce un montón de información de ustedes sin que ustedes lo sepan, sin su consentimiento".

Por su parte, Fernández habló de lo último en materia de privacidad y geolocalización de

(1) Bielli, Gastón E., "Terceros de confianza y certificación de prueba electrónica. Una nueva frontera en materia de probática", LA LEY, 03/06/2019, 1, AR/DOC/1629/2019.

(2) Acciarri, Hugo A., "Smart contracts, criptomonedas y el Derecho", LA LEY, 02/05/2019, 1, AR/DOC/1017/2019.

(3) Alvarez Echazú, María Belén, "Multa récord para Facebook: deberá pagar 5.000 millones de dólares por haber violado reglas de privacidad en Estados Unidos", Portal TRLaLey, 26 julio 2019, *http://laley.thomsonreuters.com/nota/2503*.

dispositivos móviles (4). "Tener el teléfono en el bolsillo tiene un montón de implicancias en lo que hace a nuestra privacidad", advirtió. Con esa introducción, el socio de Marval, O'Farrell & Mairal presentó el debate entre privacidad y seguridad, trajo a colación jurisprudencia nacional y extranjera, reflexionó sobre las facultades de investigación de las fuerzas de seguridad y los fiscales (5), el rol de los jueces y hasta llegó a mencionar cuestiones relativas al reconocimiento facial en la Ciudad de Buenos Aires.

El quinto panel, que llegó a ser definido como un "panel de alto riesgo", contó con la participación de Juan Corvalán, fiscal de la Ciudad Autónoma de Buenos Aires, y Johanna C. Faliero, consultora internacional en Derecho Informático, quienes cautivaron a las abogadas y los abogados con Prometea (software creado por el Laboratorio de Innovación e IA de la Facultad de Derecho de la UBA, en conjunto con el Ministerio Público Fiscal de CABA) y el derecho al anonimato.

El fiscal porteño, en primer lugar, le dijo adiós a las filas y sellos, típicas de la burocracia imprenta, y a los interminables *clicks*, apertura de ventanas y adictos del *copy-paste* (atención: a no perderse las últimas sentencias-castigo a los abogados por abuso de *copy-paste* (6)), para llevar a los presentes a una burocracia inteligente, mediante una prueba *ao vivo* del software Prometea.

A su turno, Faliero llevó al auditorio por el abuso de las técnicas de procesamiento y tratamiento de datos (*big data, data mining*, IA, *machine learning, deep learning*, etc.), los derechos modernos de protección de datos personales (derecho al olvido digital, derecho al anonimato, etc.), perfilamiento, *targeting*, los peligros de la era dataísta (fugacidad de datos, robo de identidad, hackeos, *grooming*, etc.) y, por último, a la "revolución del anonimato".

En ese contexto, Faliero aconsejó, sobre todo, resguardar nuestra identidad digital. Para ello, resaltó que debemos tener cuidado de las áreas que vamos cediendo sin darnos cuenta; no perder los beneficios sociales de la inserción de estas técnicas; tener en cuenta que la identidad digital es un derecho personalísimo, irrenunciable y fundamental en la era de datos; no renunciar al consentimiento expreso; tres derechos: derecho a la privacidad, confidencialidad, anonimato (razonable); y que las regulaciones trabajen de manera expresa la limitación sobre las técnicas de tratamientos de datos que sean riesgosos para los titulares de los datos.

El último panel sobre "Desafíos Tecnológicos para la Innovación de la Justicia" contó con la intervención de Mario Adaro, ministro de la Suprema Corte de Justicia de Mendoza, Javier Wajntraub, ex director nacional de Modernización Judicial en Ministerio de Justicia y Derechos Humanos y Luis María Palma, en ese entonces próximo a asumir como director nacional de Modernización Judicial. Todos ellos, con la moderación de Fulvio Santarelli, director Editorial y de Productos Legales LatAm Sur de Thomson Reuters.

Primero, entre reflexiones sobre el futuro del servicio de justicia (llegó a hablar de una justicia *online*), Adaro reveló grandes proyectos: la creación de una "nube federal" y la construcción de un "lago de datos". Sobre el primero, adelantó: "La idea es generar la primer nube federal de la justicia del país, donde los diversos poderes judiciales van a tener acceso a distintos servicios. Saltar al paradigma cloud va a ser un salto cualitativo, va a generar equidad, va a generar un encuentro donde desarrolladores propios se encuentren con desarrolladores de otras provincias para trabajar en común. Hasta se podría abrir a desarrolladores independientes".

Wajntraub, por su parte, compartió lo que se vino haciendo desde el Ministerio de Justicia y Derechos Humanos, que lidera Germán Garavano: un área de contención para los poderes judiciales para mejorar la prestación de los

(4) Fernández, Diego – O 'Farrell, Inés, "Privacidad en el contexto digital: la geolocalización de dispositivos móviles" Sup. Esp. LegalTech 2018 (noviembre), p. 87, AR/DOC/2377/2018.

(5) Alvarez Echazú, María belén, "Art. 131 CP: a pedido del MPF, hacen lugar a solicitud de informes a Facebook sin aviso al usuario", Portal TRLaLey, 26/07/2019, *http://laley.thomsonreuters.com/nota/2465*.

(6) Feced Abal, Francisco, "Sobre el uso (y abuso) del copy-paste", LA LEY, 27/08/2019, 6, AR/DOC/2689/2019; Alvarez Echazú, María Belén, "Otra sentencia contra el abuso del copy-paste de los abogados", Portal TRLaLey, 29/08/2019, *http://laley.thomsonreuters.com/nota/2649*.

servicios, la Agenda 2020 y la Agenda 2030. Y Palma expuso unas breves palabras sobre la tecnología y la gestión judicial: "La tecnología es una herramienta que nos ayuda a prestar mejor un servicio no es el centro de nuestras vidas". "Las técnicas cambian, los principios no. Quizá podamos, en algún momento, viajar a través de un agujero negro hasta el fin del mundo. No lo sabemos. Pero el principio es siempre dar un mejor servicio, en este caso concretamente de justicia", cerró.

Requiem para las cédulas. Automatización de las notificaciones procesales

GABRIELA FERNANDA GIL (*) Y **GABRIEL HERNÁN QUADRI** (**)

I. Palabras iniciales

Las líneas que siguen se refieren a las notificaciones procesales.

Mas precisamente, las que se practican mediante la remisión (electrónica) de cédulas.

En verdad, aquí no vamos a hablar de *cómo hacerlas*, sino que nos enfocaremos en *cómo dejar de hacerlas*.

O, al menos, *cómo lograr que los humanos* (de uno u otro lado del mostrador judicial) *ya no perdamos tiempo en confeccionarlas y remitirlas,* dejando este trabajo (engorroso, rutinario y aburrido) en manos de quienes, seguramente, lo encararán mejor y de manera más eficiente: los sistemas informáticos.

Pero, antes de ir a lo medular, primero traeremos a colación algunos conceptos que serán, luego, de utilidad para el desarrollo que sigue.

(*) Abogada, Juez Titular del Juzgado Civil y Comercial Nro. 11 Morón, Presidente Honorario de la "COMISION JUSTICIA 2020" Colegio de Abogados de Morón, Docente de grado y de posgrado.

(**) Secretario de la sala 2ª, Cámara de Apelación Civil y Comercial Morón. Director honorario del Instituto de Derecho Procesal Civil del Colegio de Abogados de Morón. Autor del Capítulo "La prueba electrónica" en el "Tratado de Derecho Procesal Electrónico", Camps, Carlos E. (dir.). Ganador del premio Accesit de la Academia Nacional de Derecho de Buenos Aires por su obra "La prueba en el proceso civil y comercial".

II. Sobre las notificaciones procesales

Las notificaciones procesales son, valga la redundancia, actos procesales; y, dentro de tal género, la diferencia específica está dada por su esencia.

Se trata de actos de comunicación, entendiendo por tales a aquellos dirigidos a poner en conocimiento a las partes o a otras autoridades de los actos de decisión (1).

Apoyándonos en lo ya expuesto, y siguiendo a Palacio, podemos decir que las notificaciones son los actos mediante los cuales se pone en conocimiento de las partes, o de terceros, el contenido de una resolución judicial (2).

Sentado ello, cabe también enfatizar en que las notificaciones, como actos procesales de transmisión, atañen al derecho de defensa en juicio (3); indudablemente, para el cabal ejercicio del derecho consagrado en el art. 18 de la Cons-

(1) COUTURE, Eduardo J., *Fundamentos del derecho procesal civil*, reimpr. inalterada, Ed. Depalma, Buenos Aires, 1997, p. 204.

(2) PALACIO, Lino E., *Derecho Procesal Civil*, 4ª ed. actualizada por Carlos Enrique CAMPS, Abeledo Perrot, Ciudad Autónoma de Buenos Aires, 2017, t. III, punto 723, Ebook disponible en Thomson Reuters Proview.

(3) MAURINO, Alberto L., *Notificaciones procesales*, 2ª ed. act. y ampl., 1ª reimp., Ed. Astrea, Buenos Aires, 2004, p. 1.

titución Nacional es necesario que la parte conozca las diversas vicisitudes del procedimiento, no solo lo que decida el tribunal, sino también aquellas cuestiones y planteamientos que vayan introduciendo los otros sujetos procesales —y que por orden del órgano jurisdiccional se bilateralicen (sistema de vistas y traslados)—.

Aunque, en realidad, cabría aquí alguna precisión pues, si el derecho de defensa debe ejercerse de conformidad con las leyes que reglamentan su ejercicio (concretamente, las leyes procesales), estas normas son las que van a determinar también la mecánica de comunicación de los actos del proceso, gozando de validez en la medida en que lo hagan razonablemente (art. 28, CN).

Introducidos así en el tema, reflexionamos también respecto a que la forma de llevar a cabo estos actos de comunicación —como es lógico— no ha sido siempre la misma, sino que ha ido evolucionando a lo largo del tiempo (4).

Es que si concebimos al proceso como un producto social es evidente que, tarde o temprano, los cambios que se vayan produciendo en el seno de la sociedad repercutirán en la forma en que se regule la discusión ante sus órganos jurisdiccionales; no sería razonable que, en una sociedad del siglo XXI, con sus propias características, reclamos y necesidades, las controversias judiciales se siguieran dirimiendo, y tramitando, del mismo modo que hace varios siglos atrás.

Ahora bien, retomando lo dicho al comienzo, tenemos que, básicamente, las notificaciones procesales implican una forma de transmitir cierta información (el contenido de una resolución), en un contexto puntual (el proceso judicial) a una o más personas determinadas; y, en sintonía con ello, podemos decir también que es conocida por todos la vertiginosa transformación que han sufrido las comunicaciones en las últimas décadas como fruto de los avances tecnológicos.

Lo que en otros tiempos fue el monopolio del contacto a distancia (la carta) ha caído en la más absoluta obsolescencia —no creemos que, hoy en día, sean muchas las personas que gestionen sus comunicaciones por vía postal—, reemplazándosela por otras formas de contacto que prácticamente absorben la totalidad de nuestras comunicaciones: los medios electrónicos.

La doctrina se ha ocupado de señalar que uno de los pasos más importantes en procura de una mayor efectividad procesal es la informatización de la administración de justicia (5) y que la incorporación de las nuevas tecnologías al ámbito judicial es una necesidad imperiosa (6).

Agregándose, en el mismo sentido, que la informática judicial es parte fundamental del proceso de modernización de la justicia con el objetivo de revertir la lentitud y morosidad en la resolución de los casos judiciales (7).

Y señalándose, también, que una de las manifestaciones más patentes de la crisis de la justicia es la obsolescencia de sus procedimientos y operaciones (8).

En tal contexto, y con relación a la modernización del servicio de justicia, surge la informática jurídica de gestión, que —según ha explicado Hitters— se ocupa básicamente de la extensión de esta disciplina a la administración de los centros de actividades jurídicas (juzgados o estudios), siendo una aplicación de la ofimática a la gestión judicial (9).

La informatización permite acelerar los trámites del proceso, aliviando a los jueces y empleados de tareas rutinarias (10).

---

(4) Maurino, Alberto L., *Notificaciones procesales*, cit., p. 5.

(5) Camps, Carlos E., "El derecho procesal y la informática", LL del 30/4/2014, p. 1.

(6) Rodríguez, Mónica S., *Algunas novedades respecto a la digitalización del procedimiento judicial y la implementación del expediente electrónico. La importancia de la modernización para una adecuada inserción en el ámbito internacional*, Microjuris MJD6534.

(7) Pagés Lloveras, Roberto M., *La informática judicial en el proceso civil*, Supl. Doct. Judicial Procesal, 2011 (mayo), p. 1.

(8) "Acerca de los aportes de la tecnología informática a una mayor eficiencia en la actividad judicial", Suplemento De Actualidad, La Ley, 3/2/2000, p. 1.

(9) Hitters, Juan C., "Influencia de la ciencia y la tecnología en el proceso", ED 127-853.

(10) Hitters, Juan C., "Influencia…", cit.

De este modo, su uso es importante para permitir a quienes toman decisiones concentrarse en sus tareas específicas (11).

Creemos que resulta imprescindible que las máquinas vengan en asistencia del operador jurídico, relevándolo de todos los cometidos en los que puedan asistirlo para permitirle ocuparse de lo realmente trascendente e insustituible.

Frente a este panorama, el ámbito de los actos de comunicación parece perfecto para que entren en juego las nuevas tecnologías.

Volvamos a su esencia: poner algo (la resolución judicial) en conocimiento de algún sujeto determinado.

Luego, si un sistema informático sabe (porque se le indica en cada caso o una sola vez como regla a utilizar para todos los supuestos idénticos) qué es lo que debe comunicarse, a quién y de qué manera, podrá ocuparse solo del resto; es una tarea por demás sencilla para las más básicas computadoras (12).

La idea, en verdad, no es novedosa y hace más de un lustro que la hemos ya dejado entrever (13); ahora, y con el auge de la automatización, parece cobrar más fuerza.

Sobre esto quisiéramos profundizar.

III. Cédulas

Empecemos por definir el vocablo, según la Real Academia Española, "cédula" (14): deriva del latín *schedŭla*, dimimutivo de *schĕda*, hoja de papel. Papel o pergamino escrito o para escribir en él algo.

Haciendo un poco de historia, la misma fuente explica que Cédula real era el Despacho del rey, expedido por algún consejero o tribunal superior, en el que se concedía una merced o se tomaba alguna providencia.

En este orden de ideas, encontramos, según los distintos regionalismos, cédulas de identidad, de habitabilidad, de vecindad (15), hipotecaria, territorialidad, urbanística, catastral, entre muchas otras; es decir que el objeto de comunicación es el "mensaje" y el "canal" es el medio papelizado "cédula", que, a través del código, forma parte del circuito comunicacional.

---

(11) Rodríguez, Claudio, "Una opinión sobre informática judicial", LL 2002-A-1240.

(12) Si el lector se detiene un segundo a pensarlo, son múltiples los ámbitos (públicos y privados) donde los actos de comunicación se llevan a cabo en forma automatizada. Operaciones de comercio electrónico, *homebanking*, obtención de turnos en oficinas públicas, entre infinitas otras situaciones.

(13) Quadri, Gabriel H., *Cavilaciones acerca de la notificación por medios electrónicos*, JA 2014-IV, 1372.

(14) Cédula. (Del lat. *schedŭla*, d. de *schĕda*, hoja de papel.) f. Pedazo de papel o pergamino escrito o para escribir en él alguna cosa. || 2. Documento en que se reconoce una deuda u otra obligación. || 3. *For.* V. Pleito de cédula. || ante díem. Papel firmado, regularmente del secretario de alguna comunidad, por el que se cita a sus individuos para juntarse al día siguiente, y en él se expresa el asunto que se ha de tratar. || de abono. La que se daba por los tribunales de Hacienda cuando el rey perdonaba a un pueblo algún débito, a fin de que el recaudador se la admitiese en data de igual cantidad. || de cambio. ant. *Com.* Letra de cambio. || de comunión. La que se da en las parroquias en tiempo del cumplimiento de iglesia, para que conste. || de diligencias. Despacho que se expedía por el Consejo de la Cámara, dando comisión a un juez para hacer alguna averiguación. || de inválidos. Orden del rey, en que concedía a algún soldado el pase a las compañías de inválidos. || de preeminencias. La que se daba a algunos individuos de un cuerpo que, habiendo servido muchos años sus oficios, no podían continuar por enfermos u ocupados, o por otras justas causas. || 2. En la milicia, orden del rey por la que se conserva en su grado el fuero militar al oficial que se retiraba. || de vecindad. Cédula personal. || en blanco. La que va firmada y se da a alguno con facultad de llenarla según le pareciere. || personal. Documento oficial que expresa el nombre, profesión, domicilio y demás circunstancias de cada vecino; acredita el pago de un impuesto, y sirve para identificar la persona. || real. Despacho del rey, expedido por algún tribunal superior, en que se concede una merced o se toma alguna providencia. Se cabeza es: *El Rey*, sin expresión de más dictados; la firma S. M.; el secretario del tribunal a que pertenece pone el refrendo; de rúbrica por algunos ministros, y por lo regular se entrega a la parte. || testamentaria. Memoria, 6.ª acep. || Real cédula. Cédula real. || Dar cédula de vida. fr. fig. y fam. que se dice de los preciados de guapos, porque parece que hacen gracia en no quitar la vida. En *Diccionario de la Lengua Española*, Real Academia Española, Decimoctava Edición, 1956; Editorial Espasa-Calpe, S. A., Madrid, España, 1 de junio de 1956.

(15) Documento oficial que expresaba el nombre, profesión, domicilio y demás circunstancias de cada individuo.

En definitiva, el núcleo conceptual radica en que el vocablo cédula informa sobre el medio material o canal en el que se concreta el acto comunicacional, seguido de la especie o particularidad informativa de que se trate, calificando la información que el papel contiene, por ejemplo, datos de identidad, catastrales, inscripción hipotecaria, etc.

El ámbito jurídico recoge el concepto de cédula de notificación originalmente bajo la modalidad papelizada.

Analizamos estos conceptos procesales desde la nueva perspectiva digital.

Podríamos decir, ¿estamos frente a un caso de eponimia (16)?

Los epónimos son aquellas palabras, normalmente nombres comunes, que provienen de un nombre propio o común. En general, son nombres de países, una actitud vital, una época determinada, un producto o una cosa.

Básicamente, designan alguna cosa con el nombre de otra.

Por eso decimos que funcionan por designación metonímica, en este caso de sustantivo común.

Cuando utilizamos la voz "cédula", nos referimos al acto comunicacional y no al canal comunicacional.

Es decir, llamamos al acto con el nombre del canal.

Comenzamos a insinuar el punto de análisis.

Cuando decimos cédula electrónica en realidad decimos papel-electrónico porque, en el binomio cédula de notificación, cédula era el canal (papel) y notificación designaba la manda o acto judicial.

Entonces, cuando nos referimos al vocablo cédula, el imaginario colectivo elaboró un conjunto de significantes jurídicos para conceptualizar la comunicación legal entre la administración de justicia (emisor) y el receptor (sujeto a quien se informa) en la voz "cédula", haciendo referencia unívoca a la notificación escrita papelizada, o cédula de notificación prevista en los códigos formales.

Identificando el vocablo "cédula o papel" con el acto comunicacional en sí mismo.

Por lo demás, y en la tramitación papelizada, la necesidad de la cédula era evidente: el juez dictaba la resolución y se la incorporaba, materialmente, al expediente en soporte papel; luego, cuando era necesario comunicarla a la parte (y salvo que esta se acercara a la sede del tribunal y se notificara personalmente), algo (un papel, es decir la cédula) debía salir de la sede del tribunal y viajar (materialmente) hasta el domicilio (también del mundo material), llevada por alguien (el notificador). De allí la necesidad de que existieran dos documentos: por un lado, la resolución judicial y, por otro, el que se confeccionaba —transcribiendo dicha resolución— y viajaba hasta el domicilio de destino.

Ahora bien, volvamos al punto de estudio: cuando hablamos de cédula electrónica o digital, sabemos que no hacemos referencia al elemento material "papel", sino al acto procesal comunicacional telemático disociado del elemento material "papel".

Sin perjuicio de ello, en la praxis foral, se reproduce el diseño de la imagen histórico-tradicional de la mentada "cédula de notificación", generándose un documento digital al solo efecto notificatorio, ahora enviado mediante el canal digitalizado.

Es indiscutible que la imagen, en especial la organización del texto, no tiene relevancia jurídica: *lo trascendente, son el conjunto de elementos informativos, que debe recibir el receptor previstos en la normativa ritual*.

El diseño de la imagen o formulario no solo carece de efectos procesales, sino que responde al costumbrismo regional, muchas veces estandarizado a los fines prácticos por los Superio-

(16) Epónimo, ma. (Del gr. ἐπώνυμος *epṓnymos*.) adj. Aplícase al héroe o a la persona que da nombre a un pueblo, a una tribu, a una ciudad o a un período o época. En *Diccionario de la Lengua Española*, Real Academia Española, Decimoctava Edición, 1956; Editorial Espasa-Calpe, S. A., Madrid, España, 1 de junio de 1956.

res Tribunales con el único objetivo de evitar la multiplicidad de formatos.

Lo cierto es que la situación comunicativa procesal, en el marco del derecho procesal digital, es el acto mediante el cual el emisor envía un mensaje a uno o varios receptores mediante el canal telemático.

El mensaje se integra con el conjunto de elementos previstos en el art. 137 del CPCCN, prescindiendo de toda formalidad que, por otra parte, vale la reiteración, surge de la praxis formularia propia del modelo papelizado.

Lo que torna innecesario elaborar documentos digitales a imagen y semejanza de los modelos formularios previstos para el soporte material al solo efecto comunicacional.

Máxime cuando la tecnología aporta modalidades superadoras y cada vez más eficientes.

IV. Automatización

Si para sentar algunos puntos de partida vamos en búsqueda de un concepto, podemos considerar que —en la Real Academia Española— el vocablo automático tiene varias acepciones.

Lo primero que detectamos (y en verdad nos sirve) es que la palabra automático proviene del griego αὐτόματος autómatos 'que actúa por sí mismo' e -ico, en el sentido de cualidad, relación o pertenencia.

Aquí ya tenemos algo: lo automático, dicho de un mecanismo o de un aparato, implica "que funciona en todo o en parte por sí solo"; hay más significados que se orientan en la misma dirección como, por ejemplo, cuando algo es "producido sin necesidad de la intervención directa del interesado".

De lo que aquí vamos a hablar, dado el objeto del presente, no es de la automatización en general de los actos procesales sino de la posibilidad de automatizar ciertos actos: los de comunicación.

Para ir afinando la exposición, podemos señalar que, como lo indica Corvalan, se llama automatización a los sistemas de inteligencia artificial menos sofisticados o menos complejos desde el punto de vista de la programación (por ejemplo, cuando entrenamos un sistema para que cuente plazos procesales). Otros sistemas más complejos utilizan aprendizaje automático para detectar patrones relevantes y, sobre esa base, tomar una decisión o elaborar una predicción. Y, por último, están los sistemas de IA más sofisticados que usan redes neuronales y pueden autoaprender, incluso, sin supervisión humana (17).

El distingo, llevado a los actos procesales, también es plausible porque nos ayuda a pensar en distintos niveles de automatización, de acuerdo con la mayor —o menor— complejidad del acto del que se trate.

En estas reflexiones, y dada la naturaleza de los actos en análisis, nos movemos dentro del primero de los aspectos aludidos.

Ahora, si se trata de referirse a la tramitación automatizada debemos detenernos, necesariamente, en el decreto 733/2018.

Su art. 1° estableció que "la totalidad de los documentos, comunicaciones, expedientes, actuaciones, legajos, notificaciones, actos administrativos y procedimientos en general, deberán instrumentarse en el sistema de Gestión Documental Electrónica – GDE, permitiendo su acceso y tramitación digital completa, remota, simple, automática e instantánea, excepto cuando no fuere técnicamente posible" a partir de las fechas en él indicadas.

A su vez, su art. 2° indicó que "todos los trámites en relación con el ciudadano deben contar con una norma que regule sus procedimientos y fije su tiempo máximo de resolución. En aquellos casos que la normativa anterior prevea la presentación de documentación en papel o el uso de papeles de trabajo, se entenderá que dicho requisito se encuentra cumplido por el uso de documentos o archivos de trabajo digitales en el sistema de Gestión Documental Electrónica -GDE", agregando que "dichos procedimientos administrativos deben ser diseña-

(17) Corvalán, Juan G., "Hacia una administración pública 4.0: digital y basada en inteligencia artificial. decreto de "tramitación digital completa", LL 2018-D, 917.

dos desde la perspectiva del ciudadano, simplificando y agilizando su tramitación".

En verdad, estas normas están dirigidas a la Administración Pública Nacional.

Pero es muy relevante, para el proceso judicial, su art. 10 en el cual se invita "al Poder Legislativo Nacional, al Poder Judicial de la Nación, a los poderes Ejecutivos, Legislativos y Judiciales de las Provincias, de la Ciudad Autónoma de Buenos Aires, así como a entes públicos no estatales y entidades bi o plurinacionales de las que la Nación o dichos gobiernos sean parte, a impulsar acciones similares que permitan la tramitación digital completa, remota, simple, automática e instantánea de todos los trámites que se realicen en la REPÚBLICA ARGENTINA".

De este modo, la automatización adquiere carta de ciudadanía en nuestro orden jurídico vigente y es perfectamente adoptable para los procesos judiciales.

V. ¿Expediente digital o proceso electrónico?

Según ha remarcado Granero, implementar un expediente digital no consiste —meramente— en digitalizar expedientes; el desafío es cambiar la mentalidad, comprender la importancia de "ser digital", pensar en digital y las cosas que ello facilita y no "pensar analógico", que es volcar a binario lo que hoy está en papel.

Agregando en ese sentido que importar mecánicamente los principios clásicos del proceso de papel para el proceso electrónico parece absolutamente inadecuado y lleva a desperdiciar una oportunidad única de mejorar el Servicio de Justicia, posibilidad que nos brindan las nuevas tecnologías (18).

Corvalan señala algo similar en el ámbito de la administración pública, pero en conceptos que aplican totalmente al proceso judicial, al decir que ya no alcanza solamente con "aplicar" las nuevas tecnologías a los problemas existentes o de mejorar sistemas informáticos para "hacer lo mismo" pero con más tecnología. Por el contrario, se trata de repensar o redefinir nuevas estrategias y formas de entender la relación entre la sociedad y la tecnología; nuevos tipos de especialización en el ámbito social que se asocien a actividades de ciencia e innovación (19).

Desde nuestra perspectiva, los problemas que, aun luego de la llegada de las nuevas tecnologías, subsisten en nuestra administración de justicia obedecen a una razón muy evidente: *el desaprovechamiento de gran parte del potencial de las TICs*.

Meditando sobre el asunto, nos parece que sería interesante repensar el problema.

Es que, en los últimos tiempos, se está poniendo el foco en el expediente digital como si esto fuera el paradigma de la innovación y la panacea para todos los males burocráticos de nuestros procedimientos.

O sea, la idea es digitalizar las actuaciones y despapelizar.

Como si el problema fuera únicamente el soporte papel.

De este modo, y al trabajar así, se trasladan a lo digital las mismas técnicas, institutos, procedimientos, métodos y rutinas de trabajo propios del soporte papel, importando soluciones pensadas y diseñadas para operar en el ámbito papelizado.

A nadie se le ocurriría, por ejemplo, pensar en un sobre para el e-mail; sencillamente porque el sobre está pensado para la comunicación epistolar.

Aquí es más o menos lo mismo.

Desde nuestro punto de vista, lo esencial es pensar cómo hacemos para informatizar el proceso y no solamente cómo hacemos para digitalizar el expediente.

Ese sería el verdadero cambio de paradigma.

Obviamente, si informatizamos el proceso, la digitalización del expediente (que desde ya es muy importante) vendrá por añadidura.

(18) Granero, Horacio R., en AA.VV. - CAMPS, Carlos E. (dir.), *Tratado de derecho procesal electrónico*, Abeledo Perrot, Buenos Aires, 2016, t. II, p. 5.

(19) Corvalán, Juan G., "Hacia una administración pública 4.0...", cit.

De lo contrario, si únicamente nos ocupamos de ver cómo despapelizamos, permaneceremos anclados a un concepto de expediente judicial concebido no ya para el siglo pasado, sino más bien para varios siglos atrás.

E incluso generando otro riesgo: que el paso del papel a lo digital engendre una nueva burocracia, ya no enfocada en los problemas del papel sino en la temática digital.

Burócratas informáticos, pero burócratas al fin.

La mirada, creemos, debe ser otra.

Nos enseña Camps que se entiende por derecho procesal electrónico al sector del derecho procesal civil que se dedica al estudio de dos materias: a) la forma en que es abordada por los órganos del Poder Judicial o arbitrales la pretensión procesal informática y b) la forma en que se desarrolla la informática jurídica judicial, entendida como las reglas de empleo de las TIC para una más adecuada prestación del servicio de justicia (20).

Y son muy claras sus reflexiones cuando contextualiza el derecho procesal electrónico con el valor eficacia, destacando que —al margen del escalón en el que se ubiquen las normas que lo integran— será la eficacia la que determine su validez; señalando que las normas de derecho procesal electrónico tienen, en teoría, todas las chances de ser las más eficaces (21).

Hacia allí, creemos, deben orientarse los esfuerzos: en buscar, usando lo electrónico como medio y no como fin, un proceso judicial más eficaz.

El más eficaz que se pueda.

Somos de la idea de que una Justicia moderna no necesita el viejo discurso donde se demanda la creación de oficinas judiciales para hacer lo mismo, de la misma manera y con más personal.

Porque la magnitud del problema hace que la solución no pase por lo cuantitativo, sino por lo cualitativo.

Porque el solo aumento de tamaño de las estructuras judiciales poco hará para solucionar un problema que es esencialmente organizativo.

Básicamente: crear más órganos para que afronten los problemas de la misma manera seguramente arrojará como resultado el pronto colapso y sobrepaso también de los nuevos organismos.

Es que los obstáculos pasan por otro lado: pasan por la forma de hacer las cosas (22).

Los programas de gestión deben, a estas alturas, superar el modelo analógico del procesador de texto y dejar de actuar como meros almacenadores de datos para ser requeridos en la confección de las estadísticas mensuales.

El expediente electrónico no es meramente la suma de escritos y documentos escaneados, sino mucho más que eso.

El reto, como lo venimos indicando, será pensar digitalmente el tráfico procesal; pensar al derecho procesal electrónico de manera sistémica (23).

Corvalán afirma que no es solo un cambio de nombre o una mera actualización de conceptos, sino que se trata de repensar una organización que será atravesada por las innovaciones más disruptivas que ha creado el ser humano en toda su historia (24).

De este modo, el derecho procesal electrónico debería abrirse paso entre las rancias estructuras burocráticas del papel, la tinta y la imprenta (25).

(20) Camps, Carlos E., en AA.VV. - CAMPS, Carlos E. (dir.), *Tratado de derecho procesal electrónico*, Abeledo Perrot, Buenos Aires, 2016, t. I, p. 2.

(21) Ver el trabajo del autor en su blog "Eficacia procesal" (https://carloscamps.com/2018/09/19/el-proceso-electronico-y-el-derecho-procesal-electronico/).

(22) Gil, Gabriela F., "La inteligencia predictiva como herramienta de eficacia en la gestión judicial", SJA 21/11/2018, 35 - JA 2018-IV.

(23) Gil, Gabriela F., "La inteligencia predictiva…", cit.

(24) Corvalán, Juan G., "Hacia una administración…", cit.

(25) Gil, Gabriela F., "La inteligencia predictiva…", cit.

Y la única manera de hacerlo, desde nuestro punto de vista, es divorciándose de aquellas instituciones y metodologías de trabajo que, quizás útiles en otros tiempos, hoy han perdido toda vigencia.

VI. Automatización y burocracia judicial: combatir el desperdicio y desaprovechamiento del capital humano

La doctrina ibérica nos llama la atención acerca de que una gran parte de la labor de los juzgados es mecánica.

Remarcando que, aunque en ello tiene una gran responsabilidad la absurda burocracia judicial, la cual refleja usos del pasado, lo cierto es que buena parte de los funcionarios judiciales invierten su tiempo utilizando modelos de los cuales simplemente modifican datos (26).

Con esto queremos significar que —hoy en día— se emplean recursos humanos para llevar a cabo labores judiciales que, sin mayor esfuerzo, podrían ser llevadas a cabo por los sistemas informáticos de manera automática; incluso el mantenimiento de esta burocracia (en lugar de utilizar sistemas de inteligencia artificial) redunda en un costo mucho mayor, como lo ha explicado Corvalan (27).

Así, el autor destaca que una de las paradojas de las organizaciones en general, y de las públicas en particular, viene dada porque los recursos humanos destinan su jornada laboral a la realización de tareas mecánicas y rutinarias. Incluso frecuentemente no hay tiempo para poner el máximo de los recursos disponibles para los problemas más complejos que no pueden ser resueltos —al menos por ahora— por sistemas de inteligencia artificial (28).

En igual lineamiento, la doctrina extranjera ha puntualizado que el futuro de la administración de justicia necesariamente involucrará un alto nivel de participación de algoritmos automáticos en cada paso del proceso, señalando incluso su potencialidad para operar en el ámbito del colapso de la administración de justicia (parecería, entonces, que el problema no es exclusivamente local) y considerándose esencial dejar de ver a las computadoras como máquinas de escribir, o calculadoras avanzadas, para empezar a verlas como algo que puede aprender de los datos y llevar a cabo tareas más complejas (29).

Así, se resalta que la automatización de los actos de procedimiento redundaría en una tramitación más rápida y en mayor eficiencia (30).

Llevando eso a nuestro ámbito, y correlacionándolo con los sistemas de gestión judicial, parece necesario que los programas superasen el modelo analógico del procesador de texto y dejaran de actuar como meros almacenadores de datos para ser requeridos en la confección de las estadísticas mensuales; señalando que ha llegado la hora de empezar a delegar, en el ámbito jurisdiccional, algunas cuestiones a las máquinas para aplicar, más efectivamente, el recurso humano, lo que no implica un mejoramiento de los sistemas conocidos ni una mera adaptación, sino que se trata de la sustitución completa del modelo burocrático digital para pasar a un sistema de comunicación inteligente y a respuestas jurisdiccionales automatizadas.

Debemos preguntarnos, entonces, si resulta lógico emplear el recurso humano para tareas sencillas cuando ello puede ser efectuado por computadores; y dejar que los humanos se ocupen de otras cuestiones.

Remarcando que, cuando los textos convencionales disponen que la tutela efectiva de derechos no podrá ser "alterada" —visión obstructiva— por las leyes que reglamenten su ejercicio, se impone que tales reglamentarios domésticos deben o deberían funcionar como facilitadores —visión propositiva—, a fin de sin-

(26) Nieva Fenoll, Jordi, *Inteligencia artificial y proceso judicial*, Marcial Pons, Madrid, 2018, p. 24.

(27) Corvalán, Juan G., "Hacia una administración…", cit.

(28) Corvalán, Juan G., "Hacia una administración…", cit.

(29) Dans, Enrique, *Algorithmic Justice, Education, and the Lawyer of the Future*, que puede consultarse en *https://lawahead.ie.edu/algorithmic-justice-education-and-the-lawyer-of-the-future/* (consulta del 24 de Julio de 2019).

(30) Nieva Fenoll, Jordi, *Inteligencia artificial*, cit., p. 25.

tonizar con las garantías reconocidas, logrando mayor accesibilidad, mayor seguridad, eficacia y eficiencia, optimizando todos recursos disponibles.

Lo que nos impone repensar ciertos trámites que se realizan en forma manual o tradicional que fueron remozados por las facilidades que permiten los procesadores de textos, pero que en esencia se siguen resolviendo como hace décadas y pasar a la "automatización digital" de los mismos, lo que importaría para la administración de justicia una mejora trascendente (31).

Dicho todo esto, estamos ya en condiciones de irnos refiriendo al meollo del asunto.

VII. *"La automatización que no miramos"*

¿Hay automatización de actos procesales hoy en día?

Claro que la hay; y de actos muy significativos.

Posemos nuestra mirada en la situación bonaerense.

El art. 124 de su Código Procesal establece que

El cargo puesto al pie de los escritos será autorizado por el Secretario, Prosecretario, Oficial mayor o el Oficial primero. La Suprema Corte o las Cámaras podrán disponer que la fecha y hora de presentación de los escritos se registren con fechador mecánico. En éste caso, el cargo quedará integrado con la firma de los funcionarios o empleados citados en el párrafo precedente. El escrito no presentado dentro del horario judicial del día en que venciere un plazo, sólo podrá ser entregado válidamente el día hábil inmediato y dentro de las cuatro (4) primeras horas del despacho.

A este respecto, ha sido pacífica —hasta ahora— la consideración del cargo como instrumento público.

Pero cuando se implementan los sistemas de presentaciones electrónicas del cargo ya dejan de ocuparse los humanos y pasan a hacerlo las máquinas; dejando de ser un instrumento público por la sencilla razón de que —ahora— no interviene más en él un oficial público y carece de firma (32).

Veamos el art. 6° del Ac. 3886/18 de la SCBA.

El mismo indica:

Las presentaciones electrónicas se tendrán por efectuadas en la fecha y hora que registre el sistema informático, el que asentará -para cada presentación- el momento exacto en que ellas ingresaron al sistema de Notificaciones y Presentaciones Electrónicas, así como los usuarios que las enviaron. En ningún supuesto se imprimirán constancias de recepción para ser agregadas al expediente. Sin embargo, luego de cada presentación el sistema generará automáticamente un comprobante con tales datos que podrá ser descargado en todo momento por los presentantes.

Si nos detenemos en la última frase vemos que el sujeto de la acción no es un humano; el sujeto es "*el sistema*"; lo cual implica todo un avance porque, cuando las normas han impuesto realización de acciones, hasta ahora siempre las colocaron en cabeza de humanos, nunca de máquinas (33).

Pero aquí es el sistema (a quien se trata como sujeto y no como objeto de la acción) quien emite la constancia.

¿Y qué dice la norma?

Que lo hace "automáticamente".

Por cierto que, del mismo modo (automáticamente), realiza lo principal: asienta el momento de ingreso de la presentación y el usuario que la envió.

Sabemos que el momento de la presentación de los escritos judiciales es un acto de suma trascendencia en el proceso porque de él de-

(31) Gil, Gabriela F., "La inteligencia predictiva…", cit.

(32) Quadri, Gabriel H., *Sistematicidad y proceso electrónico (algunas soluciones mendocinas)*, Suplemento Especial. Derecho Procesal Electrónico, Erreius, diciembre 2018, p. 117.

(33) En este sentido, su antecesora (Resolución 1872/12 de la SCBA) disponía la creación (por parte del personal del juzgado) de un trámite de cargo electrónico.

penden —muchas veces— la suerte de los derechos, al determinar su tempestividad, o no, de acuerdo con los plazos correspondientes.

Ahora, si estamos delegando en el sistema la realización (automática) de actos de semejante trascendencia (34), mutando (incluso) la esencia misma del cargo (de instrumento firmado por el oficial público a instrumento no firmado y emitido por un sistema), nada nos impide avanzar con la automatización en muchos otros actos del proceso.

Sobre este piso de marcha vamos ahora al tema central del trabajo.

VIII. Automatización y notificaciones procesales

Como decíamos en los párrafos precedentes, en esencia las notificaciones procesales implican una forma de transmitir cierta información (el contenido de una resolución), en un contexto puntual (el proceso judicial) y a una o más personas determinadas.

Ahora bien, el desembarco de los medios electrónicos en materia de actos de comunicación no ha terminado de escindirse, del todo, de las antiguas prácticas.

Hace tiempo hemos venido analizando la cuestión del impacto de las nuevas tecnologías en materia de notificaciones procesales (35).

Dado el objeto del presente, aquí vamos a observarlas desde el punto de vista de la automatización.

Es aquí donde se detecta uno de los ejemplos más palpables de la imposibilidad de abandonar los modelos y cánones tradicionales, pues al incorporar las notificaciones electrónicas a los procesos (tanto a nivel nacional como en la Provincia de Buenos Aires) se lo hizo con total apego al sistema de notificación por cédula; cambiando la cédula en papel por la cédula electrónica (con algún retoque de formato) en lugar de aprovechar las posibilidades que brinda la informática, tanto en el sentido de forma de comunicación como en cuanto a la confección de los instrumentos anoticiadores.

Esto denota un innecesario dispendio de tiempo y recursos humanos (lo que incluye los tiempos propios de los letrados —patrocinantes o apoderados— y de empleados y funcionarios judiciales) al tener que asumir la realización de labores que cualquier sistema informático puede llevar a cabo de manera totalmente automática (36).

A nivel nacional, si bien el sistema —por su diseño— es algo más sencillo para la emisión de las comunicaciones y requiere de menor trabajo rutinario, igualmente sigue dependiendo de la intervención humana. En la Provincia de Buenos Aires, mientras tanto, las exigencias de trabajo humano son mayores, tanto en lo que hace a la confección de la cédula electrónica como en lo que refiere al circuito subsiguiente.

Profundicemos un poco en este asunto, para que se lo vea con más elocuencia.

En esencia, más allá de haber abandonado el soporte papel, lo cierto es que no hemos logrado abandonar la utilización del instrumento denominado "cédula".

Vamos a trabajar, como muestreo, con la situación en los procesos civiles nacionales y de la Provincia de Buenos Aires.

En ambos casos, los Códigos Procesales conservan una directiva tajante: salvo los casos en que las notificaciones quedan a cargo del órgano judicial, las mismas deben confeccionarse por los letrados de las partes (art. 137 CPCCN, 137 CPCCBA); es necesario tener presentes,

(34) Y aun a riesgo de que presente errores. En tal sentido puede verse Bender, Agustin, *El sistema puede fallar*, Temas de Derecho Procesal, Erreius, abril 2019, p. 231. Cita digital: IUSDC286485A.

(35) Entre otros, puede verse Quadri, Gabriel Hernán, "Cavilaciones acerca de la notificación por medios electrónicos", JA 2014-IV, 1372; "El Sistema de Notificaciones Electrónicas en funcionamiento (y comenzando a crujir)", Microjuris MJ-DOC-7421-AR; "Notificaciones y presentaciones electrónicas en Provincia y Nación", Microjuris, MJ-DOC-12019-AR (doctrina audiovisual); "Sistematicidad y proceso electrónico (algunas soluciones mendocinas)", *Suplemento Especial. Derecho Procesal Electrónico*, Erreius, diciembre 2018, p. 117.

(36) Gil, Gabriela F., "La inteligencia predictiva…", cit.

especialmente, las normas reglamentarias de las notificaciones electrónicas vigentes en cada jurisdicción, en las cuales no profundizamos porque no es el punto en el que queremos centrarnos (37).

La confección de una notificación electrónica implica, básicamente, el señalamiento del sujeto al que se dirige, la selección de un domicilio y la indicación de qué es lo que se notifica; y todo esto, sorprendentemente, se lleva a cabo requiriendo de la intervención humana.

Es decir, hace falta confeccionar ciertos instrumentos (en cada jurisdicción según sus particularidades), que luego —depositados en los pertinentes casilleros virtuales— apuntan a cumplir su finalidad anoticiadora.

Aquí podrá irse despejando alguna de las razones de la ineficiencia de todo el sistema*: porque se utilizan, inadecuadamente, recursos humanos*; *porque el volumen de trabajo humano que insume la confección, confronte y emisión de estas comunicaciones es considerable*; *porque, además, al quedar las notificaciones a la espera de su realización humana, se van generando tiempos muertos procesales, que siguen dilatando la tramitación*.

¿Qué más sencillo habría que automatizar estas tareas?

La situación, incluso, es más llamativa a nivel Provincia de Buenos Aires.

Porque, aquí, al lado del sistema de notificaciones electrónicas (que es el previsto para cursarlas) funciona la llamada Mesa de Entradas Virtual (MEV).

Ocurre que, si el usuario incorpora dentro de su "set de búsquedas" una causa determinada, podrá recibir (en su aplicación del celular y solo con el retraso de algunas horas) las novedades que se produzcan en la tramitación de dicha causa, con la transcripción íntegra de las diversas providencias que se incorporan al trámite; *¡anoticiamientos que son generados de manera automática por el sistema!*

La cuestión de la automatización, amén de surgir del mismo uso del sistema, ha sido mencionado por la Suprema Corte en la RC 2234/14: "de la mera lectura del manual de la mesa de entradas virtuales (http.mev.scba.gov.ar tips. asp) surge como armar un set de búsqueda *a fin de que el sistema remita por correo electrónico las últimas novedades y resoluciones en cada una de las causas que se ingresen al mismo*, sin necesidad de revisar uno por uno los expedientes del interesado".

¿Qué tenemos entonces?

Pues horas de trabajo humano para estar confeccionando, confrontando y remitiendo notificaciones mediante el sistema oficial, en paralelo a otro sistema (también oficial) que está emitiendo alertas (y notificaciones) de manera automatizada, las cuales —si se lo piensa bien— ontológicamente tienen exactamente el mismo contenido que las cédulas electrónicas.

Podrá replicársenos las diferencias entre un sistema y otro, el hecho de que uno opera con los domicilios electrónicos y el otro con una casilla de mail, el hecho de que las cédulas se firmen y las notificaciones de la aplicación MEV no, y muchas otras cuestiones, que seguramente sean ciertas.

Pero, en realidad, el ejemplo lo evocamos solo para demostrar cómo es perfectamente posible el envío automatizado de comunicaciones, las cuales —en la práctica— pueden surtir exactamente el mismo efecto que las cursadas soporte papel; y quienes nos desempeñamos en el ámbito judicial sabemos bien que, en la generalidad de los casos, cuando la cédula es confeccionada y remitida el destinatario ya está impuesto, hace tiempo, del contenido de la resolución, pues pudo acceder a ella por intermedio de los servicios de mesa virtual.

A cómo automatizar, en las condiciones de trabajo hoy existentes, vamos a referirnos en el punto que sigue.

(37) Sobre cómo funciona el sistema y las labores (humanas) que se necesitan para que se lleve a cabo una notificación, puede verse Bielli, Gaston E. – Nizzo, Andres L., *Derecho procesal informático*, 1a ed., La Ley, Ciudad Autónoma de Buenos Aires, 2017, Ebook disponible en Thomson Reuters Proview, Capitulos XII (para la Provincia de Buenos Aires) y XV (para Nación).

IX. Realidad tangible, no futurismo: la experiencia en la práctica

Esta posibilidad de automatizar las notificaciones es algo actualmente factible en el ámbito bonaerense (38) y en varios órganos judiciales (39).

En la Provincia de Buenos Aires, al contar los magistrados con firma digital, el sistema permite cargar los domicilios de las partes a notificar (en el mismo proveído) y al tiempo de procederse a la signatura (digital) de la resolución, al usar el botón "notificar" se disparan automáticamente los anoticiamientos, los cuales cuentan con todos los datos necesarios para producir, efectivamente, la notificación electrónica.

Básicamente, y en la iniciativa llevada a cabo por el Juzgado de Primera Instancia en lo Civil y Comercial nro. 11 de Morón, el texto modelo del proveído respectivo dice así:

Morón, (fecha)

(AQUÍ EL TEXTO PRINCIPAL DE LA PROVIDENCIA)

NOTIFÍQUESE POR SECRETARÍA (arts. 34, 36 y 135 inc. 8º del CPCC), remitiéndose copia digital de la presente providencia a los domicilios electrónicos de las respectivas partes que se detallan a continuación:

Parte actora ():

(aquí se indica el domicilio electrónico)

Parte demandada y citada en garantía ():

(aquí se indica el domicilio electrónico)

Y se lo suscribe digitalmente.

A lo que se agrega que es posible, además, que la comunicación electrónica así cursada lleve documentos adjuntos o trámites asociados.

Con lo cual, la parte recibe en su domicilio la comunicación electrónica con todos los elementos necesarios y el texto del proveído que señala esta forma de notificación, aunque sin utilizar el formato (visual) cédula.

Cabe reportar, además, que hasta la fecha no se han efectuado planteos de ningún tipo e, incluso, que la Alzada del mismo Departamento Judicial ha señalado que, si bien este proceder no se ajustaba estrictamente a la normativa reglamentaria, en la medida en que no afectaba el derecho de defensa de las partes y cumplía su finalidad, nada había para objetar (40).

Esto último abre un nuevo espectro de análisis.

X. Validez jurídica

Hay una regla capital en materia de notificaciones procesales: aun cuando hubiera habido algún defecto en su realización, no cabe invalidarlas si ellas han cumplido su finalidad (art. 149 CPCCN y similar —aunque con alguna diferencia de redacción— art. del CPCCBA); en definitiva, no es más que traspolar a este ámbito el criterio rector en materia de nulidades procesales (art. 169, último párrafo, CPCCN y CPCCBA).

Esto nos demuestra que lo que importa, en definitiva, es *que el acto procesal haya cumplido su finalidad.*

He aquí la esencia.

E indudablemente, este tipo de anoticiamiento cumple su finalidad porque respeta todas las pautas que hacen al núcleo duro de la comunicación: se remiten al domicilio electrónico (como el Código Procesal lo indica), se indica su destinatario (en el texto del despacho) y llevan la resolución a comunicar íntegra,

(38) De hecho, se la está llevando a la práctica en los expedientes tramitados ante el Juzgado Civil y Comercial nro. 11 del Departamento Judicial de Morón, a cargo de la Dra. Gabriela F. Gil, coautora del presente.

(39) También en otros juzgados, como el Juzgado de Primera Instancia en lo Civil y Comercial nro. 7, del mismo Departamento Judicial, a cargo del Dr. Ramiro Tabossi Chavez (aunque en este caso con alguna diferencia en cuanto a la modalidad de trabajo y suscripción al momento de notificar); y, por lo que hemos tenido noticia, igualmente en algunos tribunales de los Departamentos Judiciales de San Martin y La Plata.

(40) C. Civ. y Com. Morón, sala 2ª, 26/3/2019, "Alvez Nicolas Fabricio Y Otro/a c/ Peidon Rodrigo Fernando Y Otros s/daños y perj".

pudiendo —tal lo dicho— también remitirse adjuntos.

La única diferencia, insistimos, es de formato (visual) y de unificación de todo lo actuado en un solo trámite, lo que era claramente inviable en el ámbito de la tramitación papelizada.

Ahora, si a ello se suma que este tipo de prácticas es la que mejor propende a la celeridad y economía procesal, queda en claro que —en una comparativa de eficacia— las notificaciones automatizadas salen ganando por donde se las mire: con once *clicks*, y en un minuto, se suplantan los múltiples pasos que conlleva la realización de una cédula electrónica en el ámbito de la Provincia de Buenos Aires (sea quien sea que la confeccione, el profesional o el juzgado).

Pero, por si esto fuera poco, existen muchas otras ventajas, de las que hablaremos en el punto que sigue.

XI. Más beneficios

Al margen de minimizar la intervención humana en la confección y emisión de los actos de comunicación, existen varias otras ventajas que reporta la utilización de esta metodología.

Hasta el momento (porque seguramente hay otras que no estemos advirtiendo), las que hemos detectado son las siguientes:

· Permite que todos los anoticiamientos se lleven a cabo en forma simultánea, lo que hace que todos los plazos comiencen a correr en forma conjunta, facilitando en gran medida su contralor y el cómputo de los términos.

· Evita la generación innecesaria de nuevos documentos electrónicos (las cédulas electrónicas), lo cual es un dato de suma trascendencia, puesto que disminuye el volumen de almacenamiento documental. El ejemplo es claro: si una resolución tenía que notificarse, supongamos, a tres partes, ello implicaba la generación de cuatro documentos (la resolución y tres cédulas). Si multiplicamos esto por todos los expedientes que tramitan en la jurisdicción bonaerense y todas las resoluciones que en ellos se notifican, nos podemos hacer una idea bastante gráfica del volumen de espacio informático que hace falta para resguardar todo esto y de cuánto espacio se ahorraría de seguirse la metodología propuesta.

· Es mucho más amigable para el operador judicial, ya que, al concentrarse en un solo trámite documental, evita la proliferación de actuaciones electrónicas (las cédulas) con la necesidad de estar ingresando, o visualizando, cada una de ellas para corroborar la efectiva realización del anoticiamiento. Aquí, insistimos, todo se concentra en un solo trámite.

XII. Volviendo algunas casillas atrás: pensar un proceso informatizado, desde su raíz

Sabemos que, hoy en día, la cuestión de la automatización —en los diversos ámbitos— prolifera de manera exponencial. No hay casi reducto de la actividad humana donde no se esté hablando de automatizar tareas o, en un nivel más alto, de potenciales usos de la inteligencia artificial.

Ciertamente, el proceso judicial no es la excepción (41).

Ahora, y desde nuestro punto de vista, aquí se da una circunstancia paradójica.

Sabemos todos que estamos viviendo un proceso de iniciativas reformistas e innovaciones a nivel normativo.

Pues bien, si nos detenemos en las dos que concitan la atención de muchos operadores jurídicos, hoy en día los Anteproyectos de reforma procesal civil y comercial de la Nación y de la Provincia de Buenos Aires, veremos que en ninguno de ellos se le ha prestado atención a este asunto.

Si leemos las Bases para la reforma nacional (42), allí no hay una sola referencia a la automatización, aunque sí se habla del expediente digital.

---

(41) Aquí son múltiples e ilustrativos los trabajos de Juan Gustavo Corvalán, especialmente la obra "Prometea. Inteligencia artificial para transformar organizaciones públicas" que puede descargarse gratuitamente en *http://dpicuantico.com/libros/prometea_oea.pdf.*

(42) *https://www.justicia2020.gob.ar/wp-content/uploads/2017/06/Bases-para-la-Reforma-de-la-Justicia-Civil-y-Comercial.pdf.*

Esto termina impactando en el Anteproyecto.

Hay varios artículos referidos a la digitalización de las actuaciones, pero si vemos lo atinente a las notificaciones, leemos en su art. 99 que "las notificaciones serán confeccionadas con apoyo del sistema informático y firmadas por funcionario judicial o, excepcionalmente, por el abogado de la parte que tenga interés en ella, por el síndico, tutor, curador, notario, perito o martillero. El juez podrá ordenar que el funcionario del juzgado suscriba los instrumentos de notificación por razones de urgencia o por el objeto de la providencia".

O sea, y en definitiva, se sigue previendo la intervención humana, con apoyo del sistema informático y firma, indicándose en el art. 98 sus requisitos.

Ahora, esto inserta una cuestión paradójica porque se prevé la firma de la notificación (básicamente, lo que hoy es la firma de la cédula), pero la constancia de notificación (lo que sería la firma del oficial notificador para la cédula en papel) la emite el sistema y esta no está suscripta ni interviene aquí ningún humano.

Es evidente cómo, con estos procederes francamente anacrónicos, se permanece anclado a instituciones propias de otros tiempos.

Desaparece la figura del oficial notificador humano, pero se mantiene la figura del creador humano del instrumento anoticiador.

A nivel Provincia de Buenos Aires la situación es más grave todavía.

En la explicación del proyecto tampoco se observan referencias generales a la automatización (salvo la atinente a la subasta electrónica) (43), y hay un acápite referido al expediente digital en el que se indica que "la tramitación electrónica es una de las herramientas fundamentales que se han incorporado para contar con un sistema adaptado a la mejora permanente del servicio de justicia".

Con relación a lo atinente a este trabajo, el art. 130 indica que "las cédulas serán confeccionadas y firmadas por los letrados o letradas de las partes o los mediadores o mediadoras o los auxiliares de justicia, que tengan interés en la notificación. Por Secretaría se rubricarán las que notifiquen embargos, medidas precautorias, entrega de bienes o modificaciones de derechos, y cuando los tribunales así lo ordenen por el objeto de la providencia" y que "los órganos judiciales realizarán de oficio la notificación electrónica de las resoluciones previstas en los apartados 3), 4), 10) y 11) del artículo 128, la que convoca a la audiencia preliminar y cualquier otra que por razones de urgencia u otro motivo se disponga por resolución fundada".

Y el art. 132 dice que "los funcionarios de los órganos judiciales confrontarán las cédulas electrónicas dentro del día hábil posterior de su ingreso al sistema informático por los interesados, remitiéndolas electrónicamente a sus destinatarios u observándolas cuando no cumplan los recaudos previstos para su validez. En las cédulas que deban cursarse en formato papel la reglamentación establecerá lo relativo a su diligenciamiento, así como los supuestos en los cuales se admitirá su generación y envío electrónicos, procurando que los oficiales diligenciadores informen electrónicamente al expediente el resultado de la diligencia".

Explicitadas las normas proyectadas, cabe detenernos para marcar varias cosas.

El hecho de que las notificaciones ya no sean confeccionadas por los letrados, sino por el órgano judicial (Anteproyecto nacional), solo implica traspasar la realización de los trabajos de unas personas a otras.

En el ámbito bonaerense, mientras tanto, se proyecta que la confección siga estando a cargo de los abogados, mediadores o auxiliares de la justicia (con algunas a cargo del órgano judicial), manteniéndose el añejo concepto de cédula y, lo más grave (dentro de lo grave), se sigue acudiendo a la institución del confronte humano (práctica que, quienes trabajamos en el Poder Judicial hace ya algunas décadas —y no tememos así estar deslizando algún dato etario propio— llevamos realizando desde que ingresamos en tribunales).

(43) O sea, se ha tenido en miras la realización de algunos actos automatizados, pero solo en el ámbito de la subasta (art. 555 y concordantes).

Ahora, y en paralelo, se pretende dar celeridad, acudiendo al mecanismo (de probada ineficacia) consistente en la imposición de un plazo al órgano judicial *¡y colocando el confronte a cargo de los funcionarios!* Es válido preguntarse, entonces, *¿la idea es que sean los secretarios o auxiliares letrados quienes se ocupen del confronte?, ¿y que lo hagan en el plazo de un día?* (presentamos nuestras excusas por esta hermenéutica, pero esto es lo que dice el artículo proyectado).

Amén de lo cual, la norma claramente desconoce el cúmulo de trabajo y actividad humana que genera la necesidad de proceder al confronte de las cédulas y el tiempo procesal que se pierde cuando se debe observar las mismas por un detalle mínimo; porque, lo aclaramos, por mejor voluntad que se ponga, el órgano judicial no puede enmendar siquiera una letra de lo que ha sido firmado electrónicamente por el letrado. Entonces, el error no puede ser corregido por el órgano judicial al momento del confronte, no quedándole otro remedio que observar la cédula. Y así comenzar el circuito nuevamente.

Entonces, observando ambas iniciativas, concluimos que —en lugar de modernizar (y proponer automatizar)— la idea es seguir haciendo lo mismo, es decir, haciendo cédulas, aunque escindiéndolas del soporte papel.

Y, para cerrar, creemos que lo fundamental es que este tipo de previsión legislativa —y la limitación que genera— no podrá zanjarse, luego, por vía reglamentaria, puesto que el texto de los artículos es bien claro acerca de cómo ha de procederse, estableciendo las directivas procesales a las que luego debe necesariamente ajustarse lo procedimental y reglamentario.

Remarcamos, en este sentido, que en la explicación del proyecto bonaerense que se preparó "un texto lo suficientemente flexible como para que, mediante la reglamentación posterior, pueda ir adaptándose a las modificaciones innovativas que puedan producirse, y que, así entonces, no requerirán, para su aprovechamiento, de una nueva reforma legislativa".

Desde nuestro punto de vista, es interesante esta posibilidad de dejar normas abiertas en el ámbito del proceso informatizado que permitan un amplio margen de operatividad reglamentaria.

Así, por ejemplo, el art. 136 bis del CPCC de Santa Cruz o el art. 70 inc. B del nuevo ritual mendocino, que deja la regulación abierta a lo que disponga el Superior Tribunal, sentando solo algunas pautas fundamentales que deben acatarse. O el ejemplo de la Provincia de Chubut, donde la Ley XIII Nº 14 modificó varios artículos de su Código Procesal con una delegación amplia hacia la reglamentación del Superior Tribunal.

Pero sucede que, en materia de notificaciones, esta amplitud en la reforma proyectada para la Provincia de Buenos Aires no parece haber sido tal, sino todo lo contrario: la reglamentación propuesta es minuciosa y, a la luz de lo que llevamos dicho, anclada a mecanismos pensados para un proceso del siglo pasado.

XIII. Conclusión

Lo que aquí intentamos significar, fundamentalmente, es la necesidad de profundizar la modernización de nuestros sistemas.

Sería imposible desconocer los avances que, hasta la fecha, se han venido dando con la movida tendiente a la implementación del expediente digital.

Pero, paralelamente, creemos que sería inconveniente pensar que con ellos se ha llegado a una meta.

Como lo hemos señalado, incluso con ejemplos de la praxis cotidiana, es perfectamente posible pensar en una tramitación que aproveche, en mayor medida, los recursos existentes (los humanos y también los informáticos).

Esto conlleva una imperiosa necesidad de repensar las instituciones del proceso para corroborar su ajuste a las exigencias, y posibilidades, de los tiempos que corren.

Ir del *expediente digital* hacia el *expediente inteligente*, como baluarte de un *proceso judicial informatizado*.

Ciertamente, la automatización ha adquirido carta de ciudadanía en nuestro ordenamiento

jurídico y va desembarcando, por su propio peso, en el ámbito judicial.

En este contexto y de acuerdo con lo que hemos argumentado, somos de la idea (y la práctica lo corrobora) que en materia de notificaciones judiciales podemos ya ir dejando de depender de la intervención humana para ponerlas en manos de los sistemas informáticos.

Permanecer ceñidos al concepto de cédulas y a su confección, confronte y firma por parte de seres humanos (sean los letrados, sean los integrantes del órgano judicial) nos parece, de acuerdo con el estado de cosas y posibilidades con las que contamos hoy en día, totalmente inconveniente.

Creemos, entonces, que mantener —en el contexto de un proceso informatizado— la institución de la cédula electrónica, y especialmente su generación con intervención humana, es una opción carente de eficacia.

No habría, entonces, mayores razones para conservar la vigencia de este tipo de documento judicial, fruto de las necesidades de otros tiempos pero ajeno a las de los tiempos que corren. Salvo, claro está, que la inercia o nuestro apego al pasado ("We ♥ cédulas", decíamos en el evento Legaltech, organizado por Thomson Reuters y que se llevó a cabo el 3 de Julio de 2019), sea tan fuerte que nos lleve a resistir el abandono.

Cerramos con una última idea: aquí hemos hablado de automatización y de automatización de algunos actos de comunicación; ciertamente, y como ya se lo ha argumentado en otro trabajo (44), no es esta la única posibilidad de automatizar determinados (no todos) actos del proceso.

Es un buen punto para seguir profundizando en el futuro; por ahora nos contentamos con estas reflexiones tendientes a repensar algunas formas de trabajo burocráticas y anacrónicas de nuestro sistema judicial en materia de notificaciones procesales.

---

(44) Gil, Gabriela F., "La inteligencia predictiva…", cit.

Impugnación de prueba electrónica. Un novedoso, dinámico y fluctuante escenario de la actividad probatoria moderna

CARLOS ORDOÑEZ (*)

I. Introducción

Atento el enorme potencial de las fuentes probatorias de origen electrónico, saber cuándo y cómo cuestionar la misma constituye sin lugar a dudas un tesoro preciado en la faena defensiva moderna (1).

La prueba electrónica nos invita a replantearnos las estrategias procesales tradicionales y a prestar un especial énfasis a cómo estos registros informáticos trasladan su influencia sobre la posición que asumen las partes en el proceso, especialmente cuando procuran fortalecer o desprestigiar este poderoso material convictivo.

Nos encontramos ante una temática tan importante que una desafortunada maniobra en este sentido podría conducirnos a falsas expectativas sobre el posible resultado de la contienda o, inclusive, a consecuencias no deseadas.

En este entuerto, existen ribetes especiales que deben ser analizados en detenimiento, dadas las ostensibles diferencias entre un documento en soporte papel (con o sin firma) y un documento electrónico, que además de poseer —o no— firma (electrónica o digital), puede exhibir características técnicas de toda índole, lo que a todas luces incidirá sobre el contenido o la entidad de los planteos que efectúen los litigantes.

Estos instrumentos telemáticos son una fuente inmensa de información y como tales, se han convertido en las estrellas más relumbrantes de la prueba electrónica, pues en su adquisición, representación, conservación, introducción, exploración y adecuada complementación, reconocimiento, negación e impugnación, reside el éxito de las contiendas modernas.

Para comprender este fenómeno debemos saber que el concepto de documento electrónico es tan amplio y abarcativo que dentro del mismo quedan englobados una gran variedad de supuestos que hacen a la prueba electrónica propiamente dicha.

Un documento electrónico es un documento cuyo soporte material es algún tipo de dispositivo electrónico o magnético y cuyo contenido esta codificado. Para su lectura, para su

---

(*) Abogado egresado de la Facultad de Derecho de la Universidad Nacional de Mar del Plata. Mediador. Doctorando en derecho. Secretario del Tribunal del Trabajo Nº 4 de Mar del Plata. Vicepresidente del Instituto Argentino de Derecho Procesal Informático.

(1) A los efectos de ahondar aún más sobre la incorporación al proceso y correspondiente valoración de las más diversas fuentes probatorias electrónicas utilizadas habitualmente por los litigantes (nos referimos a contenidos existentes en páginas web, correos electrónicos, WhatsApp, Facebook, Twitter, Instagram, YouTube, archivos locales, entre otros), recomendamos profundizar en Bielli, Gastón E. – Ordoñez, Carlos J., *La prueba electrónica. Teoría y práctica*, Thomson Reuters - La Ley, 2019.

reproducción o para su interpretación, necesitaremos también el auxilio de la tecnología disponible (2).

Molina Quiroga prefiere hablar de documento digital, definiéndolo como aquel que es conservado en formato digital en la memoria central del ordenador o en las memorias de masa y que no puede ser leído o conocido por el hombre sino como consecuencia de un proceso de traducción que hace perceptible y comprensible el código de señales digitales. Técnicamente, el documento digital es un conjunto de impulsos eléctricos que recaen en un soporte de computadora que, sometidos a un proceso, permiten su traducción al lenguaje natural a través de una pantalla, una impresora u otro periférico que genere un resultado equivalente (3).

De esta manera, cuando un juez valora bajo estas premisas una filmación, un mensaje de WhatsApp, una publicación de Facebook o Twitter, una página web, un mail, una fotografía, un audio, los registros existentes en un software, una firma electrónica, entre otros, técnicamente lo que está apreciando es un documento electrónico, con las derivaciones legales que ello implica. Esto no quiere decir que sea lo mismo un archivo de imagen que un archivo de video o de audio; o un documento no firmado que un documento signado con tecnología de firma digital o firma electrónica; o un mensaje enviado por una red local que un correo electrónico o un mensaje multimedia, etc. (4), existiendo distintas variables de estos instrumentos y no todas gozando de las mismas propiedades.

A lo largo del presente trabajo, haremos un repaso general del instituto para después sumergirnos de lleno en las situaciones más usuales con las que nos podemos encontrar y que ameritan un esfuerzo impugnativo extra o adicional del interesado para no sucumbir en el complejo entramado de información que almacenan estas fuentes probatorias.

II. La prueba electrónica. Aproximaciones

Quadri ya ha sostenido que la prueba es un medio de verificación de las proposiciones que los litigantes formulan en el juicio o, en el caso en que la ley lo autoriza (ej. arts. 163, inc. 6°, p. 2, Cód. Proc. Civ. y Com.; arts. 200 y 201, CPC Córdoba), de acreditación de los hechos conducentes para la solución del litigio; mientras tanto, si pasamos a su análisis en el marco de un proceso concreto, prueba será —vista desde el enfoque del resultado— todo motivo o razón aportados al proceso para llevar al juez el convencimiento o la certeza sobre los hechos. Probar será, entonces, la acción de aportar tales razones y motivos, en orden a dejar verificada alguna de las proposiciones formuladas en juicio; y la actividad probatoria será aquella encaminada a probar (por cierto, con un resultado contingente, pues podrá —o no— lograr su objetivo) (5).

Y coincidimos con el citado autor en que la prueba electrónica no es, en esencia, diferente a cualquier prueba en general, conforme ingresa dentro del campo más amplio de la prueba; es decir, y valga la redundancia, la prueba electrónica no es más que prueba.

En el derecho comparado español, ya el maestro Lluch ha sostenido que la expresión prueba electrónica puede definirse como la información obtenida a partir de un dispositivo electrónico o medio digital, el cual sirve para adquirir convencimiento de la certeza de un hecho o, con mayor precisión doctrinal, la información obtenida a partir de un dispositivo electrónico o medio digital, el cual sirve para formar la convicción en torno a una afirmación relevante para el proceso (6).

(2) Tanco, María Cecilia, "Actos procesales electrónicos" en Camps, Carlos E. (dir), *Tratado de Derecho Procesal Electrónico*, Editorial AbeledoPerrot, Buenos Aires, 2015, t. II, p. 209.

(3) Molina Quiroga, Eduardo, "Ley de expedientes digitales y notificaciones electrónicas judiciales", LA LEY 22/06/2011, 1 – LA LEY2011-C, 1224 – Enfoques 2012 (enero), 02/01/2012, 70.

(4) Ordoñez, Carlos J., "La prueba electrónica y su valoración en sede laboral", en Granero, H. R. (Dir.), *E-Mails, chats, WhatsApp, SMS, Facebook, filmaciones con teléfonos móviles y otras tecnologías. Validez probatoria en el proceso civil, comercial, penal y laboral*, Buenos Aires, 2019, p. 289.

(5) Quadri, Gabriel H., *La prueba en el proceso civil y comercial*, t. I, Abeledo-Perrot, Buenos Aires, 2011, p. 17.

(6) Lluch, Xavier A., *Derecho probatorio*, Editorial Bosch, Barcelona, 2012, p. 1109.

Siguiendo esa senda, nosotros definimos a la prueba electrónica como aquella prueba cimentada en la información o datos, con valor probatorio, que se encuentran insertos dentro de un dispositivo electrónico o que hubiera sido transmitida por un medio afín, a través de la cual se adquiere el conocimiento sobre la ocurrencia o no de hechos que las partes hayan afirmado como fundamento de sus derechos, o cuestionados, y que deban ser invocados dentro de un proceso judicial (7).

Ahora bien, agregamos que técnicamente está constituida por campos magnéticos y pulsos electrónicos, susceptibles de ser recolectados, acreditados, analizados y valorados por aquellos individuos que posean los conocimientos necesarios a dichos fines (8).

Y, en el marco de un proceso judicial, la prueba electrónica tiene por objeto cualquier registro que pueda ser generado dentro de un sistema informático, entendiendo por este a todo dispositivo físico (computadoras, *smartphones*, tablets, CDs, DVD, *pen drives*, etc.) o lógico, empleado para crear, generar, enviar, recibir, procesar, remitir o guardar a dichos registros que, producto de la intervención humana u otra semejante, han sido extraídos de un medio informático (9).

En este sentido, lo distintivo de la prueba electrónica es que está esencialmente vinculada a hechos o actos jurídicos ocurridos o realizados a través de medios informáticos. Es decir, resulta determinante que los hechos asuman una configuración informática.

Entonces, una fotografía, un video, una página web, un correo electrónico, una base de datos, una contabilidad en un programa de cálculo Excel –por citar algunos ejemplos–, en cualquier soporte (digital, magnético o informático), constituyen una «prueba electrónica» o «documento electrónico», aun cuando su reproducción e impugnación puedan ser diferentes (10).

III. Impugnación. Generalidades

La capital relevancia de la prueba electrónica en el pleito encuentra su razón de ser en el enorme cúmulo de información que almacenan sus registros, la cual debidamente explorada y/o robustecida permite formar convencimiento en el juez sobre la veracidad de los hechos o actos que documentan.

Este gigantesco potencial de la probática digital, como contrapartida, obliga a prestar un especial énfasis a la faz defensiva, cuyo debido abordaje asume un rol preponderante para los litigantes.

Ante todo, debemos incorporar, comprender y conocer los aspectos técnicos indispensables que caracterizan a las mismas y cómo juegan aquellos en la mayor o menor eficacia probatoria de estas modernas fuentes (11).

No se requiere que los profesionales se conviertan en expertos en ingeniería informática para poder trabajar con este tipo de probanzas, aunque si deberán internalizar el conocimiento necesario que les permita ejercer la tarea de forma eficiente, ya sea procurándose la asistencia necesaria o absorbiendo los contenidos mínimos ineludibles a tales fines.

En el ejercicio actual del derecho, cada vez es más frecuente que los letrados litigantes sean consultados sobre la ocurrencia de hechos o actos jurídicos que de alguna manera se encuentran mediados por elementos relativos a la evidencia electrónica. Ergo, para poder exponerlos adecuadamente en el marco de una acción judicial y, luego, probarlos de un modo jurídicamente relevante y, eventualmente, defenderse de este tipo de evidencia, es fundamental que los abogados posean un conocimiento acabado del medio informático que les permita explicarlo y ofrecer la prueba necesaria para fundar su posición.

(7) Bielli, Gastón E. - Ordoñez, Carlos J., *La prueba electrónica. Teoría y práctica*, La Ley, Buenos Aires, 2019.

(8) Bielli, Gastón E. - Ordoñez, Carlos J., cit.

(9) Vaninetti, Hugo A., "Preservación y valoración de la prueba informática e identificación de IP", LL 2013-C-374.

(10) Lluch, Xavier A., *Derecho probatorio*, cit.

(11) Para una mayor profundización sobre cada uno de estos aspectos véase Bielli, Gastón E. - Ordoñez, Carlos J., *La prueba electrónica. Teoria y práctica*, cit.

Asimismo, resulta trascendental saber cuáles son los mecanismos que nos proporciona el orden ritual o que mejor se ajustan al mismo para desvirtuar o restar eficacia probatoria a estas modernas fuentes.

El reconocimiento o la negación de un documento electrónico es uno de ellos, disponiendo el art. 356 del Cód. Proc. Civ. y Com. que al demandado le incumbe la carga de: "…reconocer o negar categóricamente cada uno de los hechos expuestos en la demanda, la autenticidad de los documentos acompañados que se le atribuyeren y la recepción de las cartas y telegramas a él dirigidos cuyas copias se acompañen. Su silencio, sus respuestas evasivas, o la negativa meramente general podrán estimarse como reconocimiento de la verdad de los hechos pertinentes y lícitos a que se refieran. En cuanto a los documentos se los tendrá por reconocidos o recibidos, según el caso…".

Igual peso recae sobre la contraparte en caso de que existiera reconvención o de que se le diere traslado de nuevos documentos (art. 358 Cód. Proc. Civ. y Com.).

Aunque en muchas ocasiones no es suficiente el mero desconocimiento de la prueba electrónica, sino que asimismo deviene imprescindible realizar una actividad procesal de mayor envergadura, más compleja e incluso acompañada de un debido respaldo probatorio.

Estamos hablando específicamente de la "impugnación".

Rojas efectúa un lúcido análisis de las implicancias del término "impugnación" en el plano probatorio, resaltando que no es privativo del ámbito recursivo, y así nos brinda numerosos ejemplos de su utilización práctica (impugnación de la prueba pericial o testimonial, entre otros) (12).

Asimismo, el autor citado reflexiona que se impugna para atacar, para quitarle eficacia, para restarle validez, esto es, para privar de efectos jurídicos a aquello que se está atacando, por eso es importante tener en cuenta dos aspectos básicos: por un lado, el sentido de la voz "documento" y, por otro, el sentido de la voz "impugnación", pues sobre ellos se deberá construir la elaboración necesaria a los efectos de poder demostrar en el proceso aquello que se persigue, es decir, la privación de los efectos jurídicos de aquello que se ha impugnado.

Enfocándonos en el plano de la prueba documental, vemos que el orden procesal presta un especial énfasis a la impugnación de los instrumentos públicos, reglada en el art. 395 del Cód. Proc. Civ. y Com. y nada dice de los instrumentos privados, que se encuentran huérfanos de regulación.

La aparición de los documentos electrónicos en el ámbito jurídico y su ascendiente crecimiento en la escena probatoria tornó mucho más evidente este vacío normativo, en razón de las diferentes aristas que ofrecen tales archivos, lo que trae aparejado un desarrollo peculiar y especializado de la labor impugnativa, totalmente distinto a lo que ocurría con los clásicos documentos en soporte papel.

En esta compleja empresa, debemos comprender que la fortaleza de todos los instrumentos telemáticos gira alrededor de tres ejes basilares, que son: autoría, integridad y licitud.

La autoría sirve para desdeñar quién es el autor del documento electrónico, vale decir, de quién emanó el mismo para así producir consecuencias legales de diverso tenor. La integridad apunta a descartar o eventualmente restar eficacia probatoria a aquellos documentos telemáticos que hayan sido objeto de modificaciones o adulteraciones o que carezcan de aptitud para trasmitir confianza técnica. La licitud busca confinar cualquier medio probatorio obtenido o producido en violación al orden jurídico en su conjunto, independientemente de que se trate de una norma adjetiva, sustancial o supra legal (Constitución Nacional y Tratados Internacionales de igual jerarquía) (13).

(12) Rojas, Jorge A., "Prueba documental: Redargución y adveración", en *Revista de Derecho Procesal*, 2005-2, Prueba – II, Rubinzal - Culzoni Editores, Santa fe, 2005, ps. 45-46.

(13) Para una mayor profundización sobre cada uno de estos aspectos véase Bielli, Gastón E. - Ordoñez, Carlos J., *La prueba electrónica. Teoría y práctica,* cit.

En la mayoría de los casos, en la conjunción de estos tres pilares fundantes residirá la fuerza probatoria de los mismos, de lo cual se coligen tres conclusiones de gran valor: la primera, que estamos ante tres conceptos independientes entre sí; la segunda, que podremos atacar cualquiera de ellos, sin tener necesidad de impugnar todos, para restarle eficacia probatoria al documento; y la tercera constituye una derivación de aquellas y consiste en que, en algunas ocasiones, bastará con desvirtuar solo uno para echar por tierra la prueba (v.gr. licitud).

Uno de los inconvenientes más frecuentes en la generalidad de estos instrumentos radica en que los mismos no permiten *per se* una efectiva identificación del remitente (autoría), sino que, eventualmente, solo proporcionan los datos del dispositivo donde se ha generado y remitido.

Entonces, para enervar la eficacia probatoria de una firma electrónica que se atribuya a determinada persona, la clave de la impugnación va a estar dada por controvertir la confiabilidad de los soportes y procedimientos técnicos utilizados para asociar al mismo a un usuario determinado.

Por el lado de la integridad, un aspecto a tener en consideración en una eventual impugnación es la volatilidad del formato, atento que no se requieren grandes conocimientos o habilidades para su manipulación, ni mucho menos instrumental complejo.

No todos los documentos digitales poseen las mismas propiedades técnicas. Existe una gran diversidad y grados de seguridad al respecto, por lo que tendremos que ser cuidadosos en su debida individualización y cuestionamiento. No es lo mismo atacar un documento con o sin firma digital, o uno con o sin firma electrónica.

Yendo al plano de la licitud, la regla sentada por el art. 378 del Cód. Proc. Civ. y Com. permite impugnar cualquier medio probatorio que afecte a la moral, la libertad personal de los litigantes o de terceros, o que estén expresamente prohibidos para el caso.

Todo lo dicho no hace más que poner sobre la mesa las diversas complicaciones que ofrecen los documentos electrónicos y que incluso varían en cada instrumento en particular, lo que hace que un cuestionamiento difícilmente sea similar a otro.

Tal vez los documentos electrónicos con firma digital sean el mejor ejemplo de este atolladero. Dada la fortaleza legal que gozan los mismos al contar con las presunciones de autoría e integridad, conllevan un esfuerzo defensivo complejo más similar a la impugnación de instrumento público que al ataque de un instrumento privado.

No obstante, existen muchísimos otros supuestos que también demandan una ardua labor en ese sentido.

Lo que queremos significar es que los documentos electrónicos en muchos casos requerirán un cuestionamiento especifico, más allá que el orden procesal únicamente nos constriña a negar o reconocer tales instrumentos y nada más, pues una debida impugnación de los mismos, acompañada de un andamiaje probatorio adecuado, será la única manera de restarle eficacia a estas fuentes tan poderosas.

En cuanto al momento procesal oportuno para efectuar este tipo de cuestionamientos de mayor complejidad, ante el desamparo adjetivo habrá que estarse a cada caso en particular y a las previsiones rituales referidas al cuestionamiento de prueba documental.

A modo de ejemplo, tratándose de documentos electrónicos anexados al escrito de demanda o a la contestación de la misma, no caben dudas que la etapa y el plazo pertinente para impugnar aquellos será el reglado por los arts. 356 y 358 del Cód. Proc. Civ. y Com., respectivamente.

IV. Supuestos especiales

a) *Falsedades:*

Todo documento electrónico —por diseño— es modificable dado que puede ser objeto de agregados, reformas, adulteraciones o manipulaciones de todo tipo y tenor, presentando un contexto más que delicado en el ámbito judicial al tiempo de analizar la confiabilidad del material probatorio de esta naturaleza.

Mediante una impugnación de falsedad buscaremos atacar la "integridad de la prueba" (obviamente en los casos que ello correspondiere), con el objetivo de mostrarle al juez que se encuentra frente a una fuente probatoria corrompida y que, por ende, carente de toda eficacia.

Antes de activar este andamiaje, los abogados deberán llevar a cabo tareas de investigación forense menores, tendientes a detectar posibles irregularidades técnicas en este material de probatorio.

A modo de ejemplo, podremos estudiar las propiedades del documento electrónico que tengamos en nuestro poder y así, con tan sólo hacer clic en el botón derecho del mouse, sabremos la fecha de creación del archivo, lo cual arrojará información muy útil para verificar su correspondencia con los hechos; a través de la utilización de WhatsApp Web podremos corroborar que los mensajes instantáneos que tenemos a la vista en un celular no han sido adulterados; analizando el código fuente de la página web que surge de un acta de constatación notarial chequearemos su equivalencia con el dominio original; verificando la línea móvil involucrada mediante una consulta en la web del ENACOM sabremos quién es el titular de la misma; entre otros.

En cuanto al momento oportuno para deducir este tipo de impugnaciones, habrá que estarse a cada caso en particular, por regla general, tratándose de cuestionamientos de documentos electrónicos anexados al escrito de demanda o a la contestación de la misma, no caben dudas que la etapa y el plazo pertinente para impugnar aquellos será el reglado por los arts. 356 y 358 del Cód. Proc. Civ. y Com., respectivamente.

Lo que no quita que puedan darse otros supuestos, por ejemplo, el previsto por el art. 365 del Cód. Proc. Civ. y Com. (hechos nuevos), o los establecidos por los arts. 388 (documentación en poder de una de las partes) o 389 (documentación en poder de terceros) del Cód. Proc. Civ. y Com., entre otros, que darán inicio al cómputo de un nuevo plazo impugnativo.

***b)** Firma digital:*

Un documento electrónico rubricado con firma digital válida, es decir, emitida de conformidad a las disposiciones legales y reglamentarias vigentes, presupone que dicha operatoria fue efectuada por el titular del certificado (autoría) y que el instrumento no ha sido modificado desde el momento de su rúbrica (integridad).

Ergo, si el resultado de un procedimiento de verificación de una firma digital aplicado a un documento telemático es verdadero, estas presunciones legales garantizan el no repudio por parte del firmante, tanto de la rúbrica como del contenido del instrumento.

Estas características del documento con firma digital, que respetan estándares internacionales, lo convierten en un muro probatorio prácticamente infranqueable, a prueba de cuestionamientos que dejan la faena impugnativa de los litigantes muy limitada, reducida a supuestos específicos y con consecuencias procesales —en la generalidad de los casos— bastante atenuadas.

Dentro de ellos, sobresalen todas aquellas cuestiones que hagan al ataque de validez de la firma digital y cuyos requisitos especialmente se encuentran reglados en el art. 9° de la ley 25.506 (14).

Así, una firma digital podrá ser impugnada por falta de emisión durante su periodo de vigencia, por no poder ser verificable y por carecer de un certificado emitido por un certificador licenciado, y para ello deberá desplegarse una actividad probatoria en ese sentido.

Sin embargo, en caso de prosperar ese tipo de ataques no producirán *per se* la desestimación de la prueba, sino muy por el contrario, la misma continuará siendo válida, aunque con las limitaciones propias de la firma electrónica, tal como prevé el art. 5° de la Ley de Firma Digital.

(14) Art. 9° (Ley 25.506): "Una firma digital es válida si cumple con los siguientes requisitos: a) Haber sido creada durante el período de vigencia del certificado digital válido del firmante; b) Ser debidamente verificada por la referencia a los datos de verificación de firma digital indicados en dicho certificado según el procedimiento de verificación correspondiente; c) Que dicho certificado haya sido emitido o reconocido, según el artículo 16 de la presente, por un certificador licenciado".

Todo lo expuesto pone sobre el tapete la enorme eficacia probatoria de esta fuente, cuya impugnación —en la mayoría de los supuestos— difícilmente pueda ser capitalizada satisfactoriamente por el impugnante.

Al respecto, la doctrina ha dicho que la firma digital está revestida de una serie de formalidades que le permiten contar con una presunción, asimilándola a la certificación de firma por escribano, pero con un condimento menor: la presunción es *iuris tantum* y no se debe recurrir —necesariamente— a la redargución de falsedad para su impugnación (15).

Respecto al momento pertinente para atacar estos tipos de documentos, tratándose de prueba documental, resultan aplicables los mismos conceptos que venimos viendo precedentemente.

***c)** Ilicitudes:*

Hoy en día nos encontramos ante un escenario probatorio muy particular, caracterizado por la facilidad con que los litigantes recolectan y documentan información de la realidad que los rodea, al punto tal de preconstituir prueba por sus propios medios en todo momento y lugar, sin contralor alguno del guardián de la función judicial.

Y hay que tener muchísimo cuidado con esta realidad, el procedimiento no puede convertirse en un gerenciador de datos informáticos (prueba) mal habidos y en un instigador de conductas probatorias irregulares.

En ese afán, cumple un rol significativo la actividad impugnativa desplegada por las partes, ya que la misma pondrá en evidencia el desapego legal o el agravio constitucional que motive la exclusión de la prueba y, asimismo, importará el ejercicio de una garantía que el orden normativo pone en cabeza de su titular, para que este la utilice —o no— cuando lo estime menester.

Respecto al momento procesal oportuno para deducir la misma, tratándose de prueba documental, resultan aplicables los mismos conceptos que venimos viendo "ut supra", y en torno a otros medios probatorios, habrá que estarse a cada caso en particular.

Una mención especial merece la prueba obtenida a través de un reconocimiento judicial web. Si se realiza con carácter anticipado, antes de trabarse la litis, el plazo para impugnar la prueba comenzará a correr desde que se tomó conocimiento formal de la prueba, no obsta ello la presencia de la defensora oficial en el acto. Si se lleva a cabo con carácter anticipado, pero después de trabada la litis y con la presencia del demandado, deberá ser impugnado al contestar el escrito de inicio. Idéntica oportunidad será aplicable cuando se desarrolle la prueba en la etapa pertinente.

***d)** Actas de constatación:*

Una modalidad muy usual son las actas notariales de constatación de contenido digital pasadas ante un escribano público, a fin de que el mismo de fe de la información que aprecian sus ojos y que luego será reflejada en el protocolo pertinente.

Idéntica función cumplen los reconocimientos judiciales virtuales que, si bien poseen una naturaleza totalmente distinta, en definitiva, comparten la misma esencia.

La fortaleza de estos tipos de documentos públicos reside en que los funcionarios intervinientes (v.gr. escribano o secretario), por imperio del art. 296 del Cód. Civ. y Com., darán plena fe de:

a) En cuanto a que se ha realizado el acto, la fecha, el lugar y los hechos que el oficial público enuncia como cumplidos por él o ante él hasta que sea declarado falso en juicio civil o criminal;

b) En cuanto al contenido de las declaraciones sobre convenciones, disposiciones, pagos, reconocimientos y enunciaciones de hechos directamente relacionados con el objeto principal del acto instrumentado, hasta que se produzca prueba en contrario.

Observarán el distingo que efectúa la norma, elevando a rango de instrumento público únicamente el primer supuesto contemplado y solo podrá ser atacada mediante una redargución de falsedad, y no así el segundo,

(15) Izquierdo, Carlos, G., "Recibo de sueldo digital", DT 2011 (abril), 806, IMP 2011-5, 249, Cita Online: AR/DOC/765/2011.

que al no poseer tales características bastará la mera impugnación.

Sin embargo, es interesante agregar que el Código Civil y Comercial de la Nación contiene una regulación específica de las actas notariales, que viene a complementar el régimen general expuesto.

Luego de regular los requisitos de la misma en el art. 311 del Cód. Civ. Y Com., (16) el legislador se ocupa de aclarar, en el art. 312 del Cód. Civ. Y Com., que el valor probatorio de las actas se circunscribe a los hechos que el notario tiene a la vista, a la verificación de su existencia y su estado. En cuanto a las personas, se circunscribe a su identificación si existe y debe dejarse constancia de las declaraciones y juicios que emiten.

Queda claro entonces que el escribano solo da fe de lo que tiene a la vista, cuyo conocimiento adquiere sensorialmente, ya sea de la existencia de un documento electrónico, o de la identidad de los partícipes y no así de lo que no puede apreciar con sus propios sentidos.

Siguiendo ese razonamiento, en el caso de que quisiéramos impugnar lo que el notario o el funcionario interviniente tuvo a la vista, indefectiblemente la única vía pertinente será el incidente de redargución de falsedad.

A su respecto, el art. 395 del Cód. Proc. Civ. y Com. dispone que "La redargución de falsedad de un instrumento público tramitará por incidente que deberá promoverse dentro del plazo de DIEZ (10) días de realizada la impugnación, bajo apercibimiento de tenerla por desistida. Será inadmisible si no se indican los elementos y no se ofrecen las pruebas tendientes a demostrar la falsedad. Admitido el requerimiento, el juez suspenderá el pronunciamiento de la sentencia, para resolver el incidente juntamente con ésta. Será parte el oficial público que extendió el instrumento".

Acá, a los fines del cómputo de los plazos, habrá que efectuarse un distingo según se trate de un acta de constatación efectuada ante un notario, que deberá ser presentada en las oportunamente fijadas al efecto (arts. 333, 334 y 365 del Cód. Proc. Civ. y Com.), o de un reconocimiento judicial.

En cuanto a la actividad probatoria que deberá llevarse a cabo en el incidente, la jurisprudencia ha dicho que la prueba tendiente a demostrar la falsedad de un instrumento público debe examinarse con criterio restrictivo y tener una entidad tal que produzca la convicción necesaria para revertir la presunción de legitimidad y veracidad que emana de tal instrumento, (17) no bastando para ello las meras inferencias o indicios (18).

e) Hackeo de cuenta:

Vivimos en una época de plena ebullición y masificación de las redes sociales, existe una gran variedad de ofertas en el mercado, para todas las edades y gustos, gratuitos o pagas, según las preferencias de contenido del usuario.

Quién no escuchó alguna vez en un programa de chimentos a algún famoso exculpándose de un posteo en una red social, con la justificación "me hackearon la cuenta". Aunque, lejos está de

(16) Art. 311 (CCyCN): "Las actas están sujetas a los requisitos de las escrituras públicas, con las siguientes modificaciones: a) se debe hacer constar el requerimiento que motiva la intervención del notario y, en su caso, la manifestación del requirente respecto al interés propio o de terceros con que actúa; b) no es necesaria la acreditación de personería ni la del interés de terceros que alega el requirente; c) no es necesario que el notario conozca o identifique a las personas con quienes trata a los efectos de realizar las notificaciones, requerimientos y otras diligencias; d) las personas requeridas o notificadas, en la medida en que el objeto de la comprobación así lo permita, deben ser previamente informadas del carácter en que interviene el notario y, en su caso, del derecho a no responder o de contestar; en este último supuesto se deben hacer constar en el documento las manifestaciones que se hagan; e) el notario puede practicar las diligencias sin la concurrencia del requirente cuando por su objeto no sea necesario; f) no requieren unidad de acto ni de redacción; pueden extenderse simultáneamente o con posterioridad a los hechos que se narran, pero en el mismo día, y pueden separarse en dos o más partes o diligencias, siguiendo el orden cronológico; g) pueden autorizarse aun cuando alguno de los interesados rehúse firmar, de lo cual debe dejarse constancia".

(17) CNCIV., SALA D, 4.9.73, LL 156-3; CNCIV, SALA K, 23.8.94, ED 160-553.

(18) CNCom, Sala E, "Grabovieski Víctor c/ Serebrinsky, Daniel H. s/ sumario, 14.12.2001.

ser algo ficticio, místico o cosas de "hackers", sino, muy por el contrario, es mucho más fácil de lo que parece y solo bastará manipular los programas adecuados.

Dicho ello, puede ocurrir que a uno de los litigantes le "hackeen" la cuenta de una red social y aprovechen la misma para presconstituir elementos probatorios que después sean usados en su contra en un pleito judicial. Por más alocado que suene, es al menos probable.

Ante esta posibilidad, supongamos que somos citados a un juicio y a poco que revisamos la documentación existente, nos encontramos con contenido de esta naturaleza.

¿Qué debemos hacer en esos casos? y ¿qué recaudos tenemos que tomar?

Primeramente, ante todo impugnar, obviamente dentro de los plazos legales previstos al efecto, como si se tratare de un documento más, que dicho sea de paso lo es.

En segundo término, debemos hacer la denuncia penal correspondiente y saber que el éxito de la impugnación dependerá exclusivamente del resultado de la misma, pues el juez penal es el único con competencia para averiguar si existió —o no— el ilícito.

La Corte Suprema de Justicia de la Nación, en la causa "C.G.L. s/ denuncia violación de correspondencia", con fecha 25/04/17, entendió que el acceso ilegítimo a una "comunicación electrónica" o "dato informático de acceso restringido" constituye un delito de violación de correspondencia en los términos de los arts. 153 y 153 bis del Cód. Penal (19).

No es la primera vez que el Máximo Tribunal entiende que el acceso ilegal a un medio de comunicación electrónico configura una violación de correspondencia como si fuese un correo postal tradicional. En "Díaz, Sergio Darío s/ violación correspondencia" (24/06/2014) y "N.N. s/ violación sistema informático art. 153 bis 1° párrafo" (23/06/2015), la Corte ya había establecido que "el acceso ilegítimo a una "comunicación electrónica" o a un "dato informático de acceso restringido", a los que solo es posible ingresar a través de un medio que, por sus características propias, se encuentra dentro de los servicios de telecomunicaciones que son de interés de la Nación" y deben ser investigados por la justicia federal (20).

f) Certificaciones de terceros de confianza:

Las certificaciones extendidas por terceros de confianza se caracterizan por poseer un sellado o marca de tiempo o *timestamp*, una cadena de caracteres o información codificada que identifica cuándo ocurrió un evento determinado, consolidando de forma exacta y específica la fecha y la hora del día en que sucedió (21).

Nos encontramos frente a un verdadero depositario "virtual", un custodio fiable del documento electrónico que alguna de las partes haya colocado bajo su órbita, en atención a determinados estándares de seguridad, con el objeto de procurar una mayor certeza (confianza) sobre el mismo, pero, aclaramos, no controla la legalidad de los contenidos que aloja.

Entonces, esta posibilidad de que pueda impugnarse el contenido de este documento "cer-

(19) Art. 153 (CP): "Será reprimido con prisión de quince (15) días a seis (6) meses el que abriere o accediere indebidamente a una comunicación electrónica, una carta, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, que no le esté dirigido; o se apoderare indebidamente de una comunicación electrónica, una carta, un pliego, un despacho u otro papel privado, aunque no esté cerrado; o indebidamente suprimiere o desviare de su destino una correspondencia o una comunicación electrónica que no le esté dirigida. En la misma pena incurrirá el que indebidamente interceptare o captare comunicaciones electrónicas o telecomunicaciones provenientes de cualquier sistema de carácter privado o de acceso restringido…".

Art. 153 bis (CP): "Será reprimido con prisión de quince (15) días a seis (6) meses, si no resultare un delito más severamente penado, el que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido".

(20) Delfín, Alejandra, "El hackeo de una cuenta Facebook configura un 'delito de violación de correspondencia', confirma la Corte Suprema", RDA 2017-112, 04/08/2017, 596, Cita Online: AP/DOC/622/2017.

(21) Bielli, Gastón E., "Terceros de confianza y certificación de prueba electrónica. Una nueva frontera en materia de probática", LA LEY 03/06/2019, 1, Cita Online: AR/DOC/1629/2019.

tificado", ya que la plataforma únicamente se encarga de dar certeza respecto de la existencia de un documento en tal día, hora y eventualmente, lugar.

Así, en una certificación extendida por un tercero de confianza sobre la existencia de una fotografía, por ejemplo, en una red social, la parte no podrá cuestionar la existencia de la misma, que se tendrá por probada, aunque si podrá cuestionar que la misma refiere a un perfil no fidedigno, vale decir, apócrifo.

Las enormes medidas de seguridad que poseen este tipo de plataformas, ya que la gran mayoría de los servicios disponibles en el mercado cumplen con estándares internacionales, colocan al pretenso impugnante en una situación muy similar a lo que ocurre con un documento con firma digital, pues si bien las mismas se valen del uso de tecnología de firma electrónica para materializar el sellado de tiempo, tal modalidad, siempre que se respeten los protocolos de rigor, será más que suficiente para producir el fin perseguido.

En última instancia, la prueba pericial informática nos brindará mayores detalles sobre los procedimientos técnicos empleados por la plataforma certificante y la seguridad de los mismos.

V. Reflexiones finales

Del recontó efectuado a lo largo del presente queda claro que debemos prestar una especial atención a la tarea impugnativa de la prueba electrónica.

Habrá casos sencillos en los que bastará una mera negativa de los documentos electrónicos acompañados al proceso por la parte contraria, pero en muchos casos será necesario desplegar una actividad impugnativa de mayor complejidad, fundada no solo en aspectos legales, sino también en cuestiones técnicas, cuyo debido conocimiento cumple un rol fundamental en la litigación moderna.

La prueba electrónica es una realidad de los procesos actuales, siendo sumamente importante conocer sus principales aristas y cómo interactúan las mismas con el orden jurídico vigente.

La litigación actual demanda conocimientos específicos en materia de prueba electrónica, los cuales escapan a la formación de la mayoría de los profesionales y que, a su vez, todavía no cuentan con un respaldo normativo adecuado, aumentando exponencialmente la complejidad de la tarea.

Documentos digitales. Hacia el Expediente Inteligente

RAÚL FARÍAS (*)

La enorme variedad de archivos digitales, contenedores a su vez de información documental, pueden acercar al juez y a las partes en menor tiempo y con ínfimas inversiones de dinero el conocimiento de aquello que necesitan saber.

Se hace necesario no solo analizar la viabilidad jurídica de su incorporación a expedientes completamente electrónicos y a aquellos que por estos días se trabajan en un formato híbrido, donde el papel sigue ejerciendo su fuerte gravitación cultural, sino también los recursos técnológicos que hoy se encuentran disponibles.

La mayoría de los reparos en la incorporación de información digital sin dudas responde a algo muy correcto que es la tutela de los derechos de las partes. Pero no debe perderse de vista que, en el análisis de estas cuestiones, es necesario, de alguna manera, "poner todas las cartas sobre la mesa", incluyendo aquellas que quizás transgredan los límites legales, pero que sin embargo es imperativo analizar en busca de opciones interpretativas que, sin afectar el derecho de las partes y a la espera de un cuerpo legislativo que las contenga, permitan aprovechar las enormes posibilidades que la tecnología nos ofrece.

El punto de partida en este tema es establecer una buena definición de Documento Digital. En mi opinión, la más acertada que conozco, con la pequeña salvedad que luego señalaré, es la que establece el art. 6° de la ley 25.506, de Firma Digital.

Y vale la pena analizar en detalle este texto porque de la comprensión acabada de sus términos surge un rico universo de posibilidades a la hora de manejar todo tipo de archivos digitales en el proceso.

Dicha norma dispone que "Se entiende por documento digital a la representación digital de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento o archivo. Un documento digital también satisface el requerimiento de escritura".

I. *"Representación digital de actos o hechos"*

Sin entrar en el ya saldado debate doctrinario sobre hechos y actos jurídicos y sus clasificaciones, es posible afirmar que esta parte de la norma refiere a los hechos y actos con la exten-

(*) Abogado por la Universidad de Belgrano. Posgrado Derecho de Alta Tecnología (UCA). Director Académico IT en FORES (Foro de Estudios sobre la Administración de Justicia) y fundador de los proyectos de Investigación y Educación Legal CINTEC Centro de Investigación de Nuevas Tecnologías para la Justicia y ELOC Escuela de Litigación Oral Civi. Director Académico del PEA Programa de Entrenamiento para Abogados *"Abogacía Práctica"*. Director Académico de la Diplomatura "Derecho de las Ciencias y las Tecnologías" en Estudios de Posgrado y Educación Continua de la Universidad de Belgrano.

sión que les confieren los arts. 257 (1) y 259 (2) del Cód. Civ. y Com. en cuanto fuente eficiente de situaciones o relaciones jurídicas en formato digital, esto es, con la necesaria intervención de un sistema digital binario, entendido este como el conjunto de dispositivos destinados a generar, transmitir, administrar, procesar y almacenar señales digitales (3). Así, por ejemplo, una conversación puede estar representada digitalmente en un archivo digital de audio o un contrato en uno de texto.

II. *"Con independencia del soporte utilizado para su fijación, almacenamiento o archivo"*

Esta parte de la norma alude a la forma de adquisición o creación del archivo digital que contiene a su vez el documento digital y su administración. En mi opinión, hubiera sido más acertado que en lugar de la palabra "fijación" se hubieran utilizado "creación o captura" ya que —conforme el estado de la técnica— cualquier acto o hecho representado digitalmente lo debe a que ha sido creado con un dispositivo digital en un sistema informático o bien ha sido captado o capturado con dispositivos digitales, algunos con la suficiente autonomía para traducir los datos capturados a la compresión humana (cámaras, grabadoras digitales, teléfonos inteligentes) u otros que requieren de un sistema (sondas, sismógrafos, detectores de partículas, etcétera.).

En relación con el almacenamiento o archivo, una buena aplicación del principio de "neutralidad tecnológica" en la redacción de la norma permite que puedan considerarse dentro de este universo a formas de almacenamiento cuya utilización apenas se insinuaba en el momento en que se sancionó la ley, como por ejemplo los servicios de almacenamiento en "la nube".

III. *"Un documento digital también satisface el requerimiento de escritura"*

La ley de firma digital contiene dos casos de equivalencia funcional. El primero al asimilar en su art. 3° la firma digital a la manuscrita (4) y el segundo cuando en el artículo en análisis asimila el documento digital a la escritura. Al respecto, tiene dicho la respetada doctrina que la equivalencia funcional parte de los conceptos de estructura y función y se considera que, cuando diferentes estructuras pueden desempeñar la misma función y por lo tanto pueden sustituirse entre sí, son funcionalmente equivalentes (5).

Es entonces crucial esta parte de la norma para la incorporación a expedientes electrónicos de todo tipo de documentos digitales, que solo encontrarán límites en la aptitud que tengan los sistemas de gestión judicial para admitirlos y administrarlos, o mejor aun, en los permisos otorgados por las políticas de gestión de esos sistemas, dando desde ya por descontado que lo que se describe seguidamente es técnicamente posible, conforme el estado del arte.

En efecto, la equivalencia funcional que contiene esta prescripción significa lisa y llana-

(1) Código Civil y Comercial. Art. 257.- Hecho jurídico. El hecho jurídico es el acontecimiento que, conforme al ordenamiento jurídico, produce el nacimiento, modificación o extinción de relaciones o situaciones jurídicas.

(2) Código Civil y Comercial. Art. 259.- Acto jurídico. El acto jurídico es el acto voluntario lícito que tiene por fin inmediato la adquisición, modificación o extinción de relaciones o situaciones jurídicas.

(3) La señal digital es un tipo de señal en que cada signo que codifica el contenido de la misma puede ser analizado en término de algunas magnitudes que representan valores discretos, en lugar de valores dentro de un cierto rango. Por ejemplo, el interruptor de la luz solo puede tomar dos valores o estados: abierto o cerrado, o la misma lámpara: encendida o apagada. Esto no significa que la señal físicamente sea discreta, ya que los campos electromagnéticos suelen ser continuos, sino que en general existe una forma de discretizarla unívocamente. Los sistemas digitales, como por ejemplo el ordenador, usan la lógica de dos estados representados por dos niveles de tensión eléctrica, uno alto, H y otro bajo, L (de *High* y *Low*, respectivamente, en inglés). Por abstracción, dichos estados se sustituyen por ceros y unos, lo que facilita la aplicación de la lógica y la aritmética binaria. Si el nivel alto se representa por 1 y el bajo por 0, se habla de lógica positiva y, en caso contrario, de lógica negativa. *https://es.wikipedia.org/wiki/Se%C3%B1al_digital*.

(4) Art. 3° de la ley 25.506: "Del requerimiento de firma. Cuando la ley requiera una firma manuscrita, esa exigencia también queda satisfecha por una firma digital. Este principio es aplicable a los casos en que la ley establece la obligación de firmar o prescribe consecuencias para su ausencia".

(5) Granero, Horacio, "La sanción de la Ley 26685 de Expedientes Digitales, el principio de la equivalencia funcional y la firma digital", elDial.com - CC2736.

mente que todo documento digital es también un documento escrito.

Y la importancia de ello radica en que a todo tipo de contenido digital es posible adjudicarle la categoría de "escrito", pudiendo afirmar sin ambages que, si el documento es digital, entonces está escrito. En tal sentido, si en lugar de realizar una petición en un documento digital de texto se la hace en un archivo de audio mp3, simplemente presentándose con los datos de rigor y enunciando de viva voz lo pedido, de todas formas se estaría ante un documento digital válido, desde el momento que por ser tal cumple con el requisito de escritura.

Antes de la sanción de esta norma, una foto era una foto, una filmación con audio era un registro audiovisual, un texto era un escrito. Ahora es posible darle este último carácter no solo a los documentos digitales que contengan texto, sino también a la enorme variedad de documentos que pueden generar los dispositivos digitales, cualquiera sea su contenido.

De modo tal que, más allá de las posibilidades técnicas de los sistemas de gestión judicial existentes que procesan, en general, peticiones y todo tipo de actos procesales, la norma hace viable la convivencia dentro de los llamados expedientes electrónicos de archivos digitales de audio, video, imagen, contenedores, etc., con los tradicionales escritos. Téngase presente que también todo archivo digital puede ser firmado digitalmente. Esto permite dos vías de inclusión de contenido digital en expedientes electrónicos: por un lado, como archivos individuales firmados digitalmente, es decir, sin contenido escrito ya que lo escrito le deviene de la norma y, por otro, como complementarios de archivos de texto, dado que es técnicamente posible componer documentos digitales con archivos de distinto origen, por ejemplo, al incrustar en un documento de Word archivos de audio y/o de audio y video, fotografías, planos, etc. y luego guardar ese documento en formato pdf para ser subido a la plataforma de notificaciones y presentaciones electrónicas respectivas donde será firmado digitalmente o, en su caso, electrónicamente, cumpliendo con ello el requisito de firma del instrumento, tal como lo establece en consonancia la segunda parte del art. 288 del Cód. Civ. y Com.: "…En los instrumentos generados por medios electrónicos, el requisito de la firma de una persona queda satisfecho si se utiliza una firma digital, que asegure indubitablemente la autoría e integridad del instrumento." (6)

IV. Terminología

Llegados a este punto, y habiendo utilizado reiteradamente los términos "digital" y "electrónico" sin definir ni delimitar su alcance, se advierte la necesidad de salvar uno de los obstáculos que se presentan para la asimilación de las tecnologías y su consecuente implementación en nuestra profesión, que es la falta de comprensión de algunos conceptos relacionados con la "tecnología informática"; un defecto que nos lleva a errores de apreciación y puede jugar en contra de los propios intereses y de los que representamos. Referirnos con propiedad a cuestiones tecnológicas permite moverse con mayor seguridad en el ecosistema legal-tecnológico.

Aun habiendo transcurrido ya mucho tiempo desde que esos conceptos circulan en la profusa información que tenemos a mano, nunca como en estos momentos se ha tenido que reparar más en su correcto uso; estimo que porque en el ámbito que nos ocupa, el expediente electrónico, incluso con el sub-aprovechamiento con el que está siendo concebido, se muestra como la gran herramienta movilizadora que empuja a todos al cambio, aun a los más renuentes, por la simple convicción de la fuerza.

Así, entre otros conceptos, frecuentemente se alude en forma indistinta a documentos electrónicos, digitales y digitalizados; firma electrónica y firma digital; se confunden diferentes unidades de medida y formatos de la

(6) Existe en este punto una discusión en la doctrina sobre la validez de documentos subidos a expedientes electrónicos mediante plataformas de notificaciones y presentaciones electrónicas, tanto de la SCBA como del PJN, ya que en ambos casos existe un período (en el PJN todavía perdura) en que los documentos digitales fueron firmados electrónicamente y no digitalmente como lo exige la norma del Cód. Civ. y Com. Por otra parte, a ambos tipos de firma, electrónica y digital, la ley 25.506 les adjudica distinta fuerza probatoria. Se trata de un tema importante que requiere un mayor análisis y excede este artículo.

información, redundando todo en una complicación que impide o retrasa la aceptación del medio electrónico digital, la comprensión de sus enormes posibilidades y su incorporación definitiva a nuestra vida profesional.

Quizás ayude a mejorar este panorama concentrarnos en algunos de estos conceptos que, por básicos, muchas veces pasan inadvertidos pero que son el fundamento de una correcta apreciación de los recursos con que contamos y su eventual utilización.

V. Analógico vs. Digital

Son dos conceptos importantes ya que, hasta este momento de la historia, todos los actos y hechos que se desarrollan en la vida humana parecen haber ocurrido, y aun ocurren, en el mundo analógico.

Solo a los efectos descriptivos podemos determinar dos zonas: una Analógica y otra Digital.

La zona analógica se corresponde con la existencia misma; es el lugar de los átomos y la materia. Poniendo el foco sobre lo que nos interesa y sin profundizar en un tema propio de la física, las señales analógicas provienen en general de fuentes de la naturaleza. Vivimos rodeados de este tipo de señales, como las variaciones de temperatura, de presión, velocidad, luz, sonido, etcétera.

Mediante los dispositivos electrónicos adecuados (ej. micrófono, termómetro, velocímetro, filmadora, etc.) son transformadas en señales eléctricas para su tratamiento electrónico.

Lo analógico, entonces, puede ser representado por variables continuas pero de diferentes magnitudes, como una onda.

Del otro lado, es posible caracterizar a la zona Digital como aquella donde dispositivos electrónicos digitales producen datos a partir de la menor unidad de información llamada bit (*binary digit* (7)), cuyo único valor puede ser uno o cero. De modo que una señal es digital cuando sus valores se representan con esas variables discretas en lugar de continuas, como en el caso anterior. La señal digital puede representar datos tales como imágenes, audio, texto, etc. Las señales digitales, entonces, no provienen de la naturaleza, sino que son creadas por el hombre a través de dispositivos electrónicos digitales.

Resumiendo ambos conceptos, la mayoría de las señales que representan una magnitud física (temperatura, luminosidad, humedad, etc.) son señales analógicas. Las señales analógicas pueden tomar todos los valores posibles de un intervalo; las digitales solo pueden tomar dos valores posibles (8).

Abundando en ejemplos, además de los ya mencionados, pertenecen a la zona analógica el papel, los impresos y manuscritos, las máquinas de escribir, cartas, faxes y demás registros de aparatos electrónicos analógicos. en tanto que son nativos de la zona digital todos los archivos que han sido creados o capturados por un dispositivo electrónico digital, conforme el formato que se les haya dado desde la aplicación o programa de origen. A estos archivos de primera generación se los denomina archivos digitales nativos y encontramos en este universo a los de texto, imagen, audio, video, etc. digital.

Existe una categoría intermedia, que es la de los archivos digitalizados. Estos generalmente han sido creados, grabados o capturados con dispositivos electrónicos analógicos. Debido a la imposibilidad que tienen los sistemas digitales de interpretar las señales analógicas, es necesario traducirlas a señales binarias mediante el proceso que se conoce como digitalización o conversión de señales analógicas a digitales. Básicamente, se trata de la incorporación a lo digital de registros adquiridos en la zona analógica. Tal sucede cuando digitalizamos aquella

(7) *A bit (short for binary digit) is the smallest unit of data in a computer. A bit has a single binary value, either 0 or 1. Although computers usually provide instructions that can test and manipulate bits, they generally are designed to store data and execute instructions in bit multiples called bytes. In most computer systems, there are eight bits in a byte. The value of a bit is usually stored as either above or below a designated level of electrical charge in a single capacitor within a memory device. https://whatis.techtarget.com/definition/bit-binary-digit.*

(8) Señales analógicas y digitales. Parámetros de las señales digitales. *https://www.ecured.cu/Se%C3%B1ales_anal%C3%B3gicas_y_digitales.*

cinta de video VHS para convertirla en algún formato digital, por ejemplo MP4 y guardarla en soporte DVD, o cuando escaneamos documentos o cuando convertimos nuestros discos de vinilo al formato MP3.

Sin embargo, los archivos digitalizados, una vez concluido el proceso, no dejan de ser archivos digitales nativos desde que han sido creados como un nuevo objeto digital que antes no existía. Y será fiel al contenido del registro analógico capturado, con todas sus imperfecciones en el flujo de la información (ej. videos y documentos escritos antiguos). En otros casos, contrariamente, por ejemplo en audio digital, los archivos digitales MP3 que se generan para consumo no profesional, debido a temas muy técnicos como la tasa de compresión y pérdida de datos, son de una calidad notablemente menor que sus originales en vinilo o cinta analógicos, algo que muchas personas con capacidades auditivas por encima de la media, con razón, no dejan de lamentar.

De lo dicho se advierte que, digitalizado un archivo analógico (pensemos en un antiguo documento original pasado por un scaner), su producto es un archivo digital que, firmado digitalmente, goza de la calidad de original y del valor probatorio que le asigna el art. 11 de la ley 25.506 (9). Obsérvese aquí que la ley, al aludir a "originales de primera generación", se está refiriendo al documento analógico que se reprodujo. En nuestro ejemplo, aquel antiguo documento original, sin importar si estaba escrito sobre papel, piedra o madera.

Por lo demás, existe una relación de género a especie entre los documentos electrónicos y los registros analógicos electrónicos, los archivos digitales y documentos digitalizados.

VI. Archivos y documentos digitales

Es indudable que los documentos digitales tienden a reemplazar definitivamente el soporte analógico del papel. Las razones son varias y van desde la reducción del costo y masificación del uso de dispositivos digitales capaces de captar actos o hechos, o reproducir las incontables manifestaciones del intelecto humano, hasta las ecológicas más extremas que ven en la producción del papel un precursor del cambio climático global.

En nuestro ámbito, vemos día a día que el papel tiende a degradarse por la acción de múltiples agentes, como la humedad, la luz, contaminantes, compuestos químicos de las tintas, disociación (10), etc., sin contar los espacios físicos de almacenamiento que requieren.

Los archivos digitales vienen a solucionar varios de esos inconvenientes al eliminar el papel como soporte de los documentos y asegurar, con las debidas medidas de respaldo, la perdurabilidad de la información contenida en ellos, la reducción de espacios de almacenamiento y los desplazamientos físicos del soporte de información, entre otros beneficios.

Los documentos digitales se guardan en archivos digitales o ficheros (11), creados con los programas y aplicaciones que hacen posible su posterior recuperación y transcripción al entendimiento humano.

Existe una gran variedad de archivos digitales creados por múltiples sistemas y con distintas funciones. Algunos guardan documentos escritos, expresiones de arte, mapas, esquemas, planos y la infinidad de creaciones humanas que es posible captar y plasmar en el soporte digital. Otros contienen instrucciones para ejecutar determinadas rutinas y programas, hacer funcionar computadoras o periféricos.

Pero cuando hablamos de documentos digitales, los abogados pensamos enseguida en

(9) Ley 25.506, art. 11. — Original. Los documentos electrónicos firmados digitalmente y los reproducidos en formato digital firmados digitalmente a partir de originales de primera generación en cualquier otro soporte, también serán considerados originales y poseen, como consecuencia de ello, valor probatorio como tales, según los procedimientos que determine la reglamentación.

(10) Agentes de deterioro. Instituto Canadiense de Conservación. *https://www.cncr.gob.cl/611/w3-article-56500.html?_noredirect=1*.

(11) Un archivo o fichero informático es un conjunto de bits que son almacenados en un dispositivo digital e identificado por un nombre y la descripción de la carpeta o directorio que lo contiene. A los archivos informáticos se les llama así porque son los equivalentes digitales de los archivos escritos en expedientes, tarjetas, libretas, papel o microfichas del entorno de oficina tradicional.

aquellos que usamos más a menudo en el estudio y en presentaciones judiciales, como los contenidos en archivos de texto, se trate de documentos autónomos o como parte de un email, o de documentos que digitalizamos y luego guardamos en archivos de imagen o contenedores como pdf.

Sin embargo, existen documentos digitales que, a la luz de lo comentado más arriba en punto a que cumplen con el requerimiento de escritura, pasan a formar parte de los recursos con los que es posible contar, además del consabido escrito, como medios de expresión de las pretensiones y pruebas en juicio.

Para un manejo aventajado de esta posibilidad es necesario tener en claro cuáles son esos recursos. Solo aludiendo a los más básicos, puedo mencionar los archivos de texto, audio, video, imagen, lectura y planillas de cálculo, cada uno con su propia variedad de formatos disponibles (12).

¿Pero por qué, si solo somos abogados, deberíamos conocer esos formatos de archivos en sus distintas versiones? (por ejemplo, formatos de imagen con y sin pérdida).

Pues, porque los sistemas de gestión judicial, tanto el de la Provincia de Buenos Aires como el Nacional, por citar las dos jurisdicciones más grandes del país, establecen normas y sobre todo límites al tipo de archivos que pueden ser objeto de las presentaciones, relacionados con los formatos y extensión (o "peso") en megabytes de cada uno.

Así, el Sistema de Notificaciones y Presentaciones Electrónicas de la Suprema Corte de Justicia de la Provincia de Buenos Aires, a partir del mes de noviembre de 2018 con la última actualización (5.0) del portal seguro, permite adjuntar archivos de audio MP3, video con audio MP4, imagen JPEG (todos formatos de compresión con pérdida (13)), e imagen PNG, un archivo de compresión sin pérdida. Se amplían además las versiones de archivos PDF soportadas desde la 1.3 a la 1.7 inclusive. Cabe recordar que los archivos PDF 1.4 en adelante son los que admiten firma digital (14).

En el orden nacional, la situación es menos auspiciosa ya que, si bien el Portal de Gestión de Causas del PJN se encuentra en desarrollo, existen mayores limitaciones a los formatos digitales de los archivos que es posible subir y solo para presentaciones de mero trámite y copias de escritos presentados en papel durante las 24 horas previas.

En ese sentido, se admiten únicamente tres tipos de archivos: TIFF y PDF para documenta-

(12) Texto: txt, docx, eml, html, etc.
Imágenes: jpg, png, gif, bmp, etc.
Audio: mp3, wav, wma, etc.
Video: avi, mp4, mpeg, mwv, etc.
Lectura: pdf, epub, mobi, etc.
Planillas de calculo: xls, csv.

(13) Algoritmo de compresión con pérdida se refiere a cualquier procedimiento de codificación que tenga como objetivo representar cierta cantidad de información utilizando una menor cantidad de la misma, siendo imposible una reconstrucción exacta de los datos originales. Esto es porque, en lugar de guardar una copia exacta, solo se guarda una aproximación. Esta aproximación se aprovecha de las limitaciones de la percepción humana para esconder la distorsión introducida. Estos algoritmos son de gran utilidad para guardar imágenes fotográficas que de otra manera ocuparían mucho espacio, dificultando su transmisión y almacenamiento. Un ejemplo de algoritmo con pérdida de calidad es JPEG. *https://es.wikipedia.org/wiki/Algoritmo_de_compresi%C3%B3n_con_p%C3%A9rdida*.

(14) El Sistema de Notificaciones y Presentaciones Electrónicas de la Suprema Corte de Justicia de la Provincia de Buenos Aires se encuentra muy avanzado en relación con el nacional, ya que permite la realización de todo tipo de presentaciones electrónicas, además de las notificaciones electrónicas, integrando la actuación de jueces y funcionarios de la justicia, así como a los abogados, auxiliares de la justicia y organismos públicos que intervienen en las causas, como Arba, Banco Provincia, IPS, Ministerio de seguridad de la pcia. Municipios, Colegios de Escribanos y de Abogados provinciales. Actualmente, la Autoridad Certificante del Poder Judicial de la Provincia de Buenos Aires emite certificados de Firma Digital en el marco de la ley 25.506 y su dto. reglamentario N° 2628/02 para sus funcionarios judiciales, para profesionales auxiliares de la Justicia matriculados en los Colegios de Abogados y para integrantes de otras entidades con convenios con la Suprema Corte de Justicia de la Provincia de Buenos Aires.

ción general, y para fotografías TIFF (15) y JPG, con un tope de 5 megabytes por archivo (16).

El caso de los archivos PDF (17) es llamativo porque, entre las pautas para la digitalización que publica el Consejo de la Magistratura con el fin de controlar el tamaño en megabytes de los archivos, se llama a evitar el reconocimiento óptico de caracteres (OCR *Optical Character Recognition*).

El OCR es un proceso dirigido a la digitalización de textos, los que, una vez identificados por el sistema como pertenecientes a un determinado alfabeto, se almacenan en forma de datos.

La función OCR, si bien agrega "peso" al archivo, permite conservar los datos del documento digital y esto es de gran importancia para el futuro del expediente electrónico porque, al despojar a un documento digital precisamente de lo más valioso que tiene que son los datos que moldean la información y que más tarde se convertirán en conocimiento, se transforma a ese documento en poco menos que una fotografía.

Eventualmente, esa misma imagen podrá ser "leída" con el fin de extraer aquellos datos perdidos, pero requiere de más procesos con la inversión de tiempo extra y software, muchas veces costoso. En definitva, un dispendio de recursos injustificable.

VII. El sacrificio de los datos

Sucede que seguimos concibiendo al expediente electrónico bajo el mismo esquema analógico del expediente en papel. No es algo achacable exclusivamente a quienes diseñan los sistemas de gestión judicial, sino que se encuentra incorporado culturalmente y arraigado con fuerza en cada uno de nosotros.

Lo experimentamos todos los días cuando nos sentamos frente a la computadora dispuestos a crear un documento cualquiera para presentar en un expediente que tramita, por ejemplo, en una plataforma de gestión judicial mixta, como la del PJN.

En este proceso, invertimos mucha tecnología digital: escribimos el documento, lo guardamos en un soporte local o en la nube, quizás lo recuperamos más tarde desde otra ubicación geográfica, hasta que decidimos imprimirlo.

En ese trágico momento, aniquilamos los datos, al menos para el futuro de la plataforma electrónica a la que irá a parar. Obtenemos así un papel que, sin restarle importancia, solo contiene información, porque ha sido "lavado" de datos y con pocas perspectivas de sumar conocimiento en el futuro.

Este sacrificio de los datos no solo ocurre si se imprime un documento hecho en computadora. También se verifica al escanear un documento sin OCR para subirlo al portal de gestión judicial, aún cuando ese tramo se desarrollare de manera completamente electrónica.

Eventualmente, y como comenté más arriba, esos datos se pueden recuperar, pero necesariamente con una mayor aplicación de recursos.

Todo esto responde a que no estamos mirando, no solo el expediente electrónico, sino todo nuestro trabajo desde la perspectiva de las máquinas. Cuando alguien elije hojear un largo documento con algunas hojas dobladas en las esquinas, en lugar de buscar un término dentro del mismo documento digital con las herramientas básicas de búsqueda estandarizadas en todos los sistemas, estamos sub-utilizando

(15) TIFF (*Tagged Image File Format*). Es un formato orientado al uso profesional, de muy alta resolución, y por esa razón tiende a expresarse en archivos muy pesados que pueden superar con facilidad los 5 megabytes por archivo tolerados por el sistema. En general no se aconseja su uso en plataformas web o digitales.

(16) Recomendaciones y pautas para la digitalización (escaneo) de la documentación. Consejo de la Magistratura. Poder Judicial de la Nación. Dirección General de Tecnología. *https://www.pjn.gov.ar/sistemas/pdf/00036893.Pdf.*

(17) El formato de documento portátil (PDF) se utiliza para presentar e intercambiar documentos, independiente del software, el hardware o el sistema operativo. Inventado por Adobe, PDF es ahora un estándar abierto y oficial reconocido por la Organización Internacional para la Estandarización (ISO). Los archivos PDF pueden contener vínculos y botones, campos de formulario, audio, vídeo y lógica empresarial. También soportan firma electrónica y firma digital y se visualizan fácilmente con el software gratuito Acrobat Reader DC. *https://acrobat.adobe.com/la/es/acrobat/about-adobe-pdf.html.*

los recursos de los que disponemos y volvemos a donde empezamos, a usar la computadora como una máquina de escribir.

VIII. Del expediente electrónico al Expediente Inteligente

Por estos días se viene observando un fuerte impulso en el desarrollo de las tecnologías como no hemos visto hasta ahora. Sucede que estamos asistiendo a los resultados de las investigaciones en Inteligencia Artificial (IA) que arrancaron por los años 50 del siglo pasado. Los avances y retrocesos en la búsqueda de una computadora inteligente que imitara los procesos del cerebro humano hicieron prevalecer por mucho tiempo entre la gente común la visión de los escépticos, que consideraban esta área investigativa solo como una fuente de guiones para películas del espacio antes que como una realidad para el desarrollo humano, como lo estamos comenzando a ver.

El proceso evidentemente no se dio con la velocidad que se esperaba y nos conformábamos con los algoritmos de búsqueda, los filtros anti spam, o con las respuestas de Siri, desde ya que no sin asombro, quizás porque no sabíamos que esas técnicas ignoran el significado de las palabras y realizan sus proezas tecnológicas con trucos de estadística, contando palabras o emparejando otras. Como lo asegura el decano investigador de lenguaje artificial, Yann LeCun (18), "Siri de Apple, solo intenta encajar lo que dices en una pequeña cantidad de categorías que producen respuestas previamente escritas. En realidad no entienden el texto".

Sin embargo, muchos de los resultados que se esperaban de la IA ya están presentes en nuevas aplicaciones o en la mejora de las existentes, por ejemplo en los servicios de Google a los que empieza a aplicarle IA (19).

El Expediente Electrónico es el caso de un desarrollo iniciado bajo rutinas de computación que se encargan de realizar tareas repetitivas, un conjunto de algoritmos o instrucciones encaminados a realizar operaciones muy concretas dentro del sistema, mucho más cercanas a un proceso mecánico que a uno razonado.

Pero, teniendo en cuenta lo comentado, es necesario que tal desarrollo tome un rápido giro en dirección a la incorporación de aplicaciones de IA y encaminarlo hacia un *Expediente Inteligente* que realmente aproveche los datos a escala que maneja, incluso los que proyecta manejar a futuro.

¿Cómo podría la IA transformar el expediente electrónico en un Expediente Inteligente? Como primera medida, debería abandonarse la linealidad analógica del clásico expediente papel sobre la que se edifica el electrónico y percibir al Expediente Inteligente en su realidad hipertextual (20), aquella que por virtud del poder de cálculo y análisis de datos de las máquinas permite obtener eficazmente la información necesaria mediante el acceso a las diversas fuentes disponibles. Estamos acostumbrados a ver el expediente como una carpeta que en forma lineal y secuencial contiene solo escritos, otros documentos y en ocasiones, algunas imágenes. Parte de esa visión se ha trasladado a los sistemas de gestión de expedientes electrónicos en uso. Pero el Expediente Inteligente debería admitir los diversos tipos de archivos digitales que fueran necesarios para lograr el objeto del proceso, habilitar la composición de archivos digitales reuniendo en uno varios archivos de otras fuentes, permitir enlaces a recursos externos y la constatación de su existencia por el sis-

(18) El hombre que enseña a las máquinas a entender el lenguaje. Yann LeCun utiliza una vieja idea de la inteligencia artificial para crear software que comprenda las palabras. MIT Technology Review.
https://www.technologyreview.es/s/5071/el-hombre-que-ensena-las-maquinas-entender-el-lenguaje.

(19) Google IA At Google AI, *we're conducting research that advances the state-of-the-art in the field, applying AI to products and to new domains, and developing tools to ensure that everyone can access* AI. *https://ai.google/.*

(20) El hipertexto es una estructura que organiza la información de forma no lineal. La estructura hipertextual permite saltar de un punto a otro en un texto —o a otro texto— a través de los enlaces. En lugar de leer el texto de forma continua, ciertos términos están unidos a otros mediante relaciones a través de los enlaces. Esto permite que los lectores o usuarios de un hipertexto accedan a la información que les interese de forma directa o que la busquen de acuerdo con sus propios intereses, sin tener que recorrer el texto entero paso a paso o secuencia a secuencia. Este tipo de estructura y esta forma de organizar la información es solo posible gracias a la utilización de un medio digital. *http://www.hipertexto.info/documentos/hipertexto.htm.*

tema, en tiempo real, así como realizar sugerencias y, con las debidas medidas de seguridad, permitirle ejecutar algunas tareas a partir del conocimiento que solo vaya adquiriendo desde los datos que procesa.

El Expediente Inteligente debe también favorecer la recepción de datos nuevos y la conversión en datos de la información existente a fin de darles tratamiento con inteligencia artificial (IA) a través de técnicas de *Machine Learning* (21) y *Deep Learning* (22).

Es que los sistemas de gestión judicial, a través de los expedientes electrónicos, son receptáculos naturales de datos a escala, auténticos epicentros de Big Data jurídica que, tratados con IA, pueden ofrecer interesantes prestaciones que mejoren sustancialmente el servicio de justicia.

Una enorme cantidad de peticiones, argumentaciones, fuentes de conocimiento y resoluciones conforman la experiencia que se desarrolla dentro del mecanismo llamado "proceso judicial" y la aplicación de IA puede permitirles a las computadoras aprender de esa experiencia y realizar muchas tareas en forma eficaz y eficiente.

Mediante el uso de redes neuronales (23) en técnicas de *deep learning* no supervisado, al aprender de datos no etiquetados ni estructurados se proporcionan a los sistemas la capacidad de razonar (24). Aplicado este tipo de IA a la miríada de datos jurídicos y judiciales constantemente actualizados, es posible identificar patrones que ayuden a sortear cuellos de botella y cargas puntuales de trabajo, distribuyendo de manera eficiente los recursos técnicos y humanos disponibles.

Uno de los fuertes de la IA es el manejo del lenguaje natural (NLP) que permite a las computadoras comunicarse con las personas mediante la lectura de texto, escucha de la voz hablada, su interpretación, el análisis de los sentimientos. La aplicación de esas habilidades al "Lenguaje Claro o Llano" (25) puede significar un enorme paso cualitativo en la comunicación de resoluciones judiciales al ciudadano como destinatario principal del servicio de justicia.

La incorporación de IA a los sistemas de gestión judicial a traves del Expediente Inteligente debe ir acompañada de la necesaria información y capacitación de los actores del derecho en punto a despejar miedos y fantasmas referidos a las consecuencias negativas sobre el trabajo. En esencia, la IA automatiza el aprendizaje y el descubrimiento de patrones repetitivos a través del análisis de datos. Por eso se dice de la IA que es distinta del trabajo de robots ya que, en lugar de automatizar tareas manuales, realiza tareas computarizadas a escala, para lo cual

(21) El *machine learning* es un método de análisis de datos que automatiza la construcción de modelos analíticos. Es una rama de la inteligencia artificial basada en la idea de que los sistemas pueden aprender de datos, identificar patrones y tomar decisiones con mínima intervención humana. *https://www.sas.com/es_ar/insights/analytics/machine-learning.html.*

(22) Murnane, Kevin, "What Is Deep Learning And How Is It Useful?", Forbes. "*Deep learning carries out the machine learning process using an artificial neural net that is composed of a number of levels arranged in a hierarchy.*

Deep learning has attracted a lot of attention because it is particularly good at a type of learning that has the potential to be very useful for real-world applications".

https://www.forbes.com/sites/kevinmurnane/2016/04/01/what-is-deep-learning-and-how-is-it-useful/#5817c5c1d547.

(23) Una red neuronal es un procesador distribuido en paralelo de forma masiva con una propensión natural a almacenar conocimiento experimental y convertirlo en disponible para su uso. Asemeja al cerebro en dos aspectos: el conocimiento se adquiere por la red mediante un proceso de aprendizaje y las fuerzas de conexión interneuronal, conocidas como ponderaciones sinápticas, se utilizan para almacenar el conocimiento. *https://www.ibm.com/support/knowledgecenter/es/SSLVMB_sub/statistics_mainhelp_ddita/spss/neural_network/nnet_whatis.html#fntarg_1.*

(24) Hao, Karen, "The AI technique that could imbue machines with the ability to reason. Yann LeCun, Facebook's chief AI scientist, believes unsupervised learning will bring about the next AI revolution", Jul 12, 2019, MIT Technology Review.

https://www.technologyreview.com/s/613954/the-next-ai-revolution-will-come-from-machine-learnings-most-underrated-form/.

(25) Sobre Lenguaje llano vea la jornada del CINTEC "Lenguaje llano en la comunicación jurídica" realizada en el Colegio de Abogados de la Ciudad de Buenos Aires el 10 de agosto de 2017.

https://forescintec.wordpress.com/2017/08/30/lenguaje-llano-en-la-comunicacion-juridica-jornada/.

la investigación humana sigue siendo un pilar fundamental en la configuración del sistema y en la elección de las preguntas correctas.

La carrera en el uso de IA ya ha comenzado en todo el mundo con las más diversas aplicaciones, como la detección de fraudes, recomendaciones de clientes, gestión de relaciones con el público, puesta en marcha de servicios, apoyo en tareas y formación, análisis de texto, taxonomías lingüísticas, enrutamiento y priorización de la información, monitoreo de riesgos, creación de datos estructurados a partir de conjuntos de datos no estructurados. Esos son solo algunos pocos ejemplos de la cantidad de tareas que se pueden asignar a la IA en un entorno de Big Data como el tratado hasta aquí.

De no aprovecharse al máximo las potencialidades tecnológicas en la gestión y análisis de la información que diariamente se produce en esa gran cantera de datos llamada Tribunales, nos estaríamos perdiendo una extraordinaria oportunidad para mejorar la Justicia.

Por eso considero una buena práctica de los sistemas que manejan grandes volúmenes de datos —llámense tribunales o estudios jurídicos— el estar preparados para este momento y los que se avecinan, capturando, administrando y guardando *datos* y no solo mera información.

El expediente electrónico debe necesariamente desplegar sus alas y volar como un Expediente Inteligente.

Yo creo que ese es su destino (26).

---

(26) "*You may say that I'm a dreamer, but I'm not the only one*". John Winston Lennon.

Los terceros de confianza en la contratación electrónica

GASTÓN E. BIELLI (*)

I. Introducción

Venimos definiendo en el pasado las certificaciones emanadas por portales terceros de confianza como aquellos sistemas informáticos accesibles vía web, ya sean públicos o privados, que mediante la implementación de tecnologías tales como la firma electrónica, el sellado de tiempo (*timestamp*), conexiones seguras y mecanismos de depósito electrónico –en forma conexa y en atención a determinados estándares de seguridad— hacen las veces de certificadores y depositarios de documentos electrónicos pasibles de atestiguar la ocurrencia de hechos u actos jurídicamente relevantes suscitados de forma mundo virtual y, consecuentemente, revestirlos del necesario valor probatorio a fin de eventualmente procurar ser introducidos, como prueba instrumental, a un proceso judicial (1).

Y en ese preliminar esbozo hemos establecido, a su vez, que surgen como una solución al problema de la fugacidad de la prueba electrónica, (conforme, en muchos casos, puede ser suprimida sin dejar rastros en cuestión de segundos, mediante unos pocos clics) y en razón de la imposibilidad temporal de recurrir, a veces, a la diligencia de un notario público de forma urgente con el objeto de procurar una constatación sobre un hecho acaecido en el mundo virtual (en ciertos lapsos de tiempo, como puede ser un fin de semana) (2).

Aclarado lo anterior, en el presente artículo intentaremos efectuar una mera aproximación al estudio de la figura del tercero de confianza a partir de su enfoque históricamente primigenio, es decir, en materia de contratación electrónica.

Es así que, en la legislación española, dicha figura tuvo originaria aplicabilidad a raíz de la falta de confianza que las partes poseían las unas en las otras, en sus relaciones jurídicas contractuales y electrónicas. Y ante esta circunstancia, y para el caso particular, la solución que ha encontrado la ley española es evitar dejar en mano de una de las dos partes la garantía y prueba de la celebración de un contrato o

(*) Maestrando en Derecho Procesal (UNR). Secretario de la Comisión de Informática del Colegio de Abogados de la Provincia de Buenos Aires (ColProBA). Presidente del Instituto Argentino de Derecho Procesal informático. Presidente de la Comisión de Derecho Informático del Colegio de Abogados de Lomas de Zamora. Docente (UNLZ).

(1) Bielli, G. E., "Terceros de confianza y certificación de prueba electrónica. Una nueva frontera en materia de probática", Diario La Ley, 6 de junio de 2019, cita online: AR/DOC/1629/2019.

(2) A fin de profundizar sobre el campo específico de la prueba electrónica, su incorporación al proceso y la correspondiente acreditación y valoración, como así también la utilidad práctica de los terceros de confianza, recomendamos la obra: Bielli, G. E. - Ordoñez, C. J., *La prueba electrónica. Teoría y práctica*, Thomson Reuters - La Ley, Buenos Aires, 2019.

de la existencia de un hecho acaecido virtualmente, por lo que acude a crear una figura ajena a ambas, un tercero (de confianza) para que reciba, custodie y ponga fecha a dicha prueba (3).

Lo trataremos de forma subsiguiente.

II. La contratación electrónica

Para profundizar el estudio de los terceros de confianza sobre la materia en tratamiento es necesario partir de la concepción, ya tradicional, de contrato electrónico.

Groover Dorado nos esboza una precisa definición al decir que se constituyen como acuerdos de voluntad cuya celebración se perfecciona sin la presencia física de las partes contratantes y a través del uso de medios electrónicos (4).

En dicha senda, los contratos electrónicos forman actualmente una (no tan nueva) tendencia dentro de las ciencias jurídicas que ha surgido ante el auge global del *e-commerce*, el cual se ha desarrollado y expandido rápidamente en los últimos años a través de la utilización de los medios tecnológicos y la Internet. Son concebidos ante la necesidad de documentar y establecer de manera clara y precisa las obligaciones entre las partes materializadas por el medio, permitiendo acelerar y facilitar el intercambio de bienes y servicios entre individuos y, consecuentemente, eliminar barreras geográficas.

Ya en nuestro entramado normativo, la recepción de la contratación electrónica se encuentra establecida en nuestro Código Civil y Comercial de la Nación, conforme regula en el Cap. 3 del Título III de su Libro Tercero, a las modalidades especiales de los contratos de consumo (arts. 1104 al 1116), dentro de los cuales incluye a los contratos celebrados a distancia.

En primer lugar, el art. 1105 establece que los mismos se perfeccionan sin la presencia física y simultánea de las partes, a través de la utilización de medios postales, electrónicos, telecomunicaciones, así como servicios de radio, televisión o prensa.

En lo relativo al empleo de medios electrónicos en los contratos a distancia, el art. 1106 señala que siempre que en este Código o en leyes especiales se exija que el contrato conste por escrito, este requisito se debe entender satisfecho si el contrato con el consumidor o usuario contiene un soporte electrónico u otra tecnología similar.

Ahora bien, ante el contexto actual, ha surgido la necesidad de establecer mecanismos idóneos para la custodia y protección de los documentos generados a través de esta nueva metodología de transacción comercial y, en especial, en lo relativo a la certificación de dichos documentos, con la finalidad de que puedan ser utilizados como medio probatorio ante cualquier eventual litigio que surja de la celebración del mismo. Y es precisamente aquí donde revisten virtual importancia los terceros de confianza.

III. Tercero de Confianza. Su utilidad en el caso de la contratación electrónica

En el marco de la contratación electrónica, el tercero de confianza actúa como un agente externo y ajeno a la relación contractual existente entre dos o más partes y es elegido de mutuo acuerdo por los interesados a los fines de que reciba, archive, custodie y ponga fecha al documento que demuestra la celebración de un contrato electrónico (5).

Revisten la naturaleza jurídica de ser meros depositarios, en razón que involucran la recepción y custodia de documentos electrónicos, lo

(3) Llopis, J. C., "Los terceros de confianza y los notarios ¿son lo mismo?", recuperado de: *http://www.notariallopis.es/blog/i/1319/73/los-terceros-de-confianza-y-los-notarios-son-lo-mismo.*

(4) Groover Dorado, J., "Los contratos electrónicos de consumo en el Derecho Argentino", SAIJ. Sistema Argentino de Información Jurídica, 26 de octubre de 2016, Id SAIJ: DACF160582.

(5) Ya a nivel local han existido antecedentes acerca del empleo de estas herramientas en materia de contratos electrónicos de compraventa. Podemos mencionar el caso de la suscripción con firma electrónica de un boleto sobre un lote localizado en la Prov. de San Luis, siendo que el documento fue posteriormente certificado en la *blockchain* de Bitcoin. La operación fue llevada a cabo por el estudio Bildenlex Abogados en base a la plataforma proporcionada por la empresa Signatura. Ver más en: *https://www.iproup.com/blockchain/1194-firma-digital-contrato-inteligente-app-Exclusivo-se-firmo-en-Argentina-la-primera-operacion-inmobiliaria-en-blockchain.*

cual puede subsumirse en el art. 1356 del Cód. Civ. y Com. (6). Es así que, respecto a las partes con las empresas brindadoras del servicio, se celebra, efectivamente, una modalidad de contrato de depósito oneroso (7).

Su marco normativo local específico está dado por el reciente Decreto 182/19, modificatorio del anterior Decreto regulador de la Ley 25.506 de Firma Digital, que vino a establecer una primaria concepción de los terceros de confianza y cómo devendrá su aplicación práctica en la Argentina (8).

Reiteramos, entonces, que lo esencial de este tipo de servicio está fundamentado por la conservación, custodia y autenticación de cualquier declaración de voluntad realizada en formato electrónico por medio de sistemas informáticos y diversas tecnologías (firma electrónica, *timestamp*, *blockchain*, biometría y/o muchas otras dependiendo de la plataforma web seleccionada por las partes), incluyendo el cumplimiento de los protocolos electrónicos internacionales de seguridad necesarios (9).

Motivado a lo anterior, en la actualidad existen diversas empresas que ofrecen sus servicios a través de sus portales web para la protección, validación y certificación de contratos electrónicos y otros documentos similares (10).

IV. El contrato electrónico celebrado bajo la órbita del tercero de confianza. Emanación y prueba

Los documentos electrónicos "certificados" (11) y emanados a través de dichos terceros de confianza constituyen instrumentos que establecerán inicialmente la validez y autenticidad de los actos o hechos jurídicos contenidos en los mismos, siendo factible su acompañamiento o presentación en cualquier proceso judicial como prueba documental y requiriéndose únicamente su valoración por parte del juez respectivo a través del correspondiente dictamen pericial informático. Y este será el medio probatorio por excelencia que confirmará la robustez del sistema originador de las firmas electrónicas conjuntamente con el cumplimiento de los estándares técnicos necesarios que aseguren la integridad y autenticidad de los aludidos instrumentos.

Ahora bien, a los fines de evaluar su valor probatorio, resulta necesario hacer énfasis y

(6) Art. 1356 CCCN. Hay contrato de depósito cuando una parte se obliga a recibir de otra una cosa con la obligación de custodiarla y restituirla con sus frutos.

(7) Aunque ciertamente es válido decir que la mayoría de estos portales proveen certificaciones gratuitas a sus usuarios, en mayor o menor medida.

(8) El art. 36 del decreto mencionado entiende por Servicio de Confianza al servicio electrónico prestado por un tercero de confianza relativo a: 1. La conservación de archivos digitales. 2. La custodia de declaraciones de voluntad realizadas en formato electrónico, contratos electrónicos, y toda otra transacción que las partes decidan confiar a un tercero depositario. 3. La notificación fehaciente de documentos electrónicos. 4. El depósito de declaraciones de voluntad realizadas en formato electrónico. 5. La operación de cadenas de bloques para la conservación de documentos electrónicos, gestión de contratos inteligentes y otros servicios digitales. 6. Los servicios de autenticación electrónica. 7. Los servicios de identificación digital. 8. Otras prestaciones que determine el Ente Licenciante.

A su vez, el art. 37 del anexo establece que, localmente, podrán brindar servicios de confianza las personas humanas, jurídicas, consorcios, entes públicos, entes públicos no estatales, de acuerdo a los procedimientos, estándares y condiciones que determine la Secretaría de Modernización Administrativa de la Secretaría de Gobierno de Modernización de la Jefatura de Gabinete de Ministros.

Cabe destacar, que las normas comentadas, delimitaron la figura del tercero de confianza en términos similares a la legislación española, pero con mayor amplitud, al enunciar expresamente a los diferentes servicios prestados por los terceros de confianza y facultando incluso a la autoridad competente, a incluir otras actividades dentro de dichos servicios.

(9) Sobre los aspectos técnicos que revisten dichos portales web, nos remitimos a lo ya tratado con anterioridad en: Bielli, G. E., "Terceros de confianza y certificación de prueba electrónica. Una nueva frontera en materia de probática", Diario La Ley, 6 de junio de 2019, cita online: AR/DOC/1629/2019.

(10) Solo a título ilustrativo, se pueden mencionar las siguientes empresas que ofrecen sus servicios como terceros de confianza en materia contractual: la empresa española Logalty (*https://www.logalty.com*) o Signaturit (*https://www.signaturit.com/es*) y, a nivel local, Signatura (*https://signatura.co/*).

(11) Es menester acotar que la certificación de estos documentos a través de un tercero de confianza no les otorga el carácter de instrumento público toda vez que los portales no reúnen los requisitos exigidos en el art. 290 del Cód. Civ. y Com., como es la participación de un notario u oficial público dando fe de la existencia de las declaraciones vertidas.

remitirnos nuevamente a las normas generales que regulan lo relativo a la prueba de los actos jurídicos contenidas en el Código Civil y Comercial de la Nación.

En primer lugar, el art. 284 del mencionado cuerpo normativo señala que, si la ley no exige una forma determinada para la exteriorización de la voluntad de las partes, estas pueden utilizar la modalidad que estimen conveniente conforme, por lo general, se materializara a través de un documento.

Luego, el art. 286 establece que la expresión escrita puede tener lugar por instrumentos públicos, o por instrumentos particulares firmados o no firmados, excepto en los casos en que determinada instrumentación sea impuesta. Puede hacerse constar en cualquier soporte, siempre que su contenido sea representado con texto inteligible, aunque su lectura exija medios técnicos.

Aquí es importante agregar que la firma constituye un elemento de vital importancia en materia documental y específicamente contractual, en razón de que con ella se demuestra la autoría del instrumento respectivo.

Y sobre este aspecto, el art. 288 expresa que la firma prueba la autoría de la declaración de voluntad expresada en el texto al cual corresponde. Debe consistir en el nombre del firmante o en un signo. En los instrumentos generados por medios electrónicos, el requisito de la firma de una persona queda satisfecho si se utiliza una Firma Digital que asegure indubitablemente la autoría e integridad del instrumento.

Con la disposición legal comentada, nuestra legislación consagró a la Firma Digital como mecanismo de suscripción por excelencia sobre documentos digitales.

Y en base a este postulado, ya hemos reiterado en varias ocasiones que actualmente existe una divergencia de criterios a nivel doctrinario sobre la eficacia jurídica de la firma electrónica como elemento de validez de los documentos electrónicos (12).

Por nuestro lado, adherimos a la tesitura amplia mediante la cual se sostiene que dicha materia corresponde ser evaluada por el juzgador, en clara alusión a lo establecido por el art. 319 del Cód. Civ. y Com.

Dicho artículo establece que el valor probatorio de los instrumentos particulares debe ser apreciado por el juez ponderando, entre otras pautas, la congruencia entre lo sucedido y narrado, la precisión y claridad técnica del texto, los usos y prácticas del tráfico, las relaciones precedentes y la confiabilidad de los soportes utilizados y de los procedimientos técnicos que se apliquen.

Es importante resaltar, a tenor de las disposiciones legales antes comentadas, que para nosotros la firma electrónica es receptada en nuestra legislación de fondo y que únicamente en un proceso judicial puede ser desvirtuado el valor probatorio de un documento electrónico suscripto mediante dicha tecnología, toda vez que, en cada oportunidad, el juez de la causa deberá evaluar todos los aspectos involucrados sobre la robustez de los sistemas originantes por medio del peritaje informático (como ser la infraestructura tecnológica, el cumplimiento de los requerimientos y protocolos de seguridad que avalen y certifiquen a los documentos electrónicos en cuestión entre otras consideraciones técnicas).

Entonces reiteramos que, en virtud de lo expuesto, a la luz de la legislación argentina, los documentos suscritos con firma electrónica y

(12) Según la doctrina, existe un criterio restrictivo que pondera a la Firma Digital como la única metodología de suscripción equiparada a la firma ológrafa o manuscrita, por lo que los documentos digitales con firma electrónica constituyen instrumentos particulares no firmados. El criterio doctrinario más amplio, afirma que el Código Civil y Comercial de la Nación y la Ley y 25.506 de Firma Digital se complementan en esta materia y que, en consecuencia, debe entenderse que dichos documentos suscriptos firma electrónica si están efectivamente firmados, correspondiendo posteriormente al juez analizar cada caso en particular, a los efectos de determinar la mayor o menor fuerza probatoria de los subtipos de firma electrónica según la infraestructura tecnológica que los respalde y en razón del artículo 319 del CCCN. (Batista, A., "¿Están legalmente 'firmadas' las presentaciones electrónicas efectuadas en el Sistema de Notificaciones y Presentaciones Electrónicas de la Suprema Corte de la Provincia de Buenos Aires?", elDial, 06/07/2017, citar: elDial DC233C).

certificados por quienes ofrecen sus servicios como terceros de confianza a través de sus respectivos portales web deben ser considerados documentos electrónicos firmados.

En este mismo orden de ideas, y de conformidad con lo previsto por el art. 1019 del Cód. Civ. y Com., los contratos pueden ser probados a través de todos los medios idóneos que permitan demostrar su existencia, según las reglas de la sana crítica y de acuerdo con lo establecido por las leyes procesales, salvo en aquellos casos en los que una disposición legal específica requiera de un medio probatorio especial.

Asimismo, el art. 1020 dispone que, en los casos de los contratos en los cuales se requiera de alguna formalidad para su prueba, pueden utilizarse otros medios probatorios en el supuesto de que exista imposibilidad de obtener la prueba una vez cumplida la formalidad respectiva o si existe el principio de prueba instrumental o comienzo de ejecución.

Y dicha norma señala, además, que se considera principio de prueba instrumental cualquier instrumento que emane de la otra parte, de su causante o de parte interesada en el asunto que haga verosímil la existencia del contrato.

No obstante, resulta pertinente aclarar que el principio de prueba no es un medio probatorio de por sí, en razón que solo corrobora la certeza de la existencia del contrato y no constituye una prueba del mismo como hecho jurídico. Por tal motivo, la parte interesada que alega la existencia de un contrato, aun cuando cuente con el principio de prueba, puede hacer valer cualquier otro medio probatorio (13).

En resumidas cuentas, sobre la base de las normas comentadas se puede afirmar que los contratos electrónicos certificados por terceros de confianza pueden ser presentados en el marco de un pleito judicial e ingresarán a este siempre y de manera primaria como un principio de prueba instrumental; correspondiéndole al juez respectivo valorar dicha prueba mediante el análisis de todo el otro caudal probatorio generado por las partes en general y a través de los peritajes informáticos que hubieran sido requeridos sobre los documentos y la infraestructura generadora. Y si como resultado de dicho peritaje quede demostrada su autenticidad en el juicio, el contrato electrónico respectivo debe ser considerado instrumento privado a tenor de lo establecido por el art. 287 del Cód. Civ. y Com.

V. Acompañamiento como medio probatorio en un proceso judicial

Al constituir el contrato certificado por el tercero de confianza una prueba documental, regirá lo dispuesto por el art. 333 del Cód. Proc. Civ. y Com. al establecer que, con la demanda, la reconvención o la contestación, las partes deben acompañar la prueba documental, así como todas las demás pruebas de las que dispongan (14).

Recordemos que la regla general en materia de prueba documental reside en que las partes tienen que acompañar todos los documentos que intenten utilizar como respaldo de sus pretensiones, siempre y cuando los mismos se encontraren en su poder en ese momento. Y conforme ello, resulta indispensable el acompañamiento del documento electrónico en su formato original, donde se consagre el material probatorio.

(13) Leiva Fernández, L. F. P., en Alterini, J. H. (Dir.), *Código Civil y Comercial comentado. Tratado exegético*, 2ª ed., Thomson Reuters - La Ley, Bs. As., t. V, p. 325.

(14) El art. 333 del Cód. Proc. Civ. y Com. establece: "Con la demanda, reconvención y contestación de ambas, deberá acompañarse la prueba documental y ofrecerse todas las demás pruebas de que las partes intentaren valerse. Cuando la prueba documental no estuviere a su disposición, la parte interesada deberá individualizarla, indicando su contenido, el lugar, archivo, oficina pública o persona en cuyo poder se encuentra. Si se tratare de prueba documental oportunamente ofrecida, los letrados patrocinantes, una vez interpuesta la demanda, podrán requerir directamente a entidades privadas, sin necesidad de previa petición judicial, y mediante oficio en el que se transcribirá este artículo, el envío de la pertinente documentación o de su copia auténtica, la que deberá ser remitida directamente a la secretaría, con transcripción o copia del oficio. Si se ofreciera prueba testimonial se indicará qué extremos quieren probarse con la declaración de cada testigo. Tratándose de prueba pericial la parte interesada propondrá los puntos de pericia".

Ahora bien, en el caso de que sea necesario presentar en el juicio un contrato electrónico en dicho carácter, surge la interrogante de cuáles son los requisitos que debe cumplir esta prueba documental y cómo debe ser acompañada con la demanda o su contestación, ampliación, reconvención o en la etapa procesal que corresponda, a los fines de que sea admitido por el juzgador.

Nosotros ya hemos procurado una metodología apropiada de incorporación al sostener que el documento (mayormente materializado en formato .pdf) debe ser acompañado mediante un CD o DVD (no regrabable a fin de que quede determinada la integridad del documento y cerrando la correspondiente sesión de grabado).

Aclaramos que, como paso previo a la realización de esta tarea, deberemos chequear el *hash* de dicho archivo (15).

En este orden de ideas, es recomendable que en el escrito que contenga la demanda, reconvención o contestación se incluya la siguiente información respecto al contrato electrónico certificado por el tercero de confianza (16):

- Título del documento.

- Fecha y hora de la certificación (17).

- Identificación completa del tercero de confianza que suscribió en forma electrónica el certificado respectivo, como así también la dirección o URL de la página web de la cual se obtuvo la certificación respectiva (18).

- Los datos de las partes intervinientes en la contratación electrónica.

- Código de verificación del documento.

- IPs desde las cuales se efectuaron las suscripciones del documento (19).

- Los datos de los navegadores utilizados para la generación de las firmas electrónicas (20).

- *Hash* del documento electrónico (21).

- Cualquier otra información que se hubiere consignado en la certificación emitida por el tercero de confianza.

VI. Conclusiones

1) A través del presente esbozo hemos intentado establecer un marco introductorio local para la utilización de los terceros de confianza en materia de contratación electrónica, siendo que constituyen una figura jurídica mediante la cual se ha permitido establecer un mecanismo efectivo para la certificación de los documentos

(15) Ya hemos definidlo al "*hash*" como una cadena alfanumérica hexadecimal generada a partir de la aplicación de un algoritmo que debe identificar de manera inequívoca un determinado documento electrónico, de tal manera que el menor cambio realizado sobre el mismo sea rápidamente detectado y visualizado. Puede verificarse en forma online a través de diferentes sitios web de acceso público como *https://md5file.com/calculato*r o en forma local descargando una aplicación como bien puede ser "MD5 & SHA Checksum Utility" mediante el sitio *http://descargar.cnet.com/MD5-SHA-Checksum-Utility/3000-2092_4-10911445.html*. Bielli, G. E., "Los mensajes de WhatsApp y su acreditación en el proceso civil", La Ley, 29/10/2018, cita online: LL AR/DOC/1962/2018.

(16) Aclaramos que la gran mayoría de la información surgirá a través del certificado emanado por el tercero de confianza.

(17) "Debe expresarse de acuerdo a la hora vigente en la República Argentina, aun cuando la certificación indique la hora del lugar en donde se encuentre el servidor del tercero de confianza o utilice la hora UTC (Coordinate Universal Time). El UTC es el principal estándar o notación del horario, mediante el cual, los países regulan y sincronizan los relojes y el tiempo. Como ejemplo se puede acotar, que, para Buenos Aires, la hora ´11:00:00 -0300´ corresponde a la hora 11:00:00 con 3 horas menos respecto de la hora universal UTC. El - 0300 se utiliza para expresar la diferencia horaria. Entonces, cuando en Bs. As. el reloj marca 11 hs, UTC marca 14 hs o 2 pm." (Fuente: *https://es.wikipedia.org/wiki/Tiempo_universal_coordinado*).

(18) Ejemplo: Logalty, S.L. es una empresa inscripta en el Registro Mercantil de Madrid, tomo 22.055, folio 60, hoja M-393.315. Es considerado un prestador cualificado de servicios de confianza, conforme al Reglamento (UE) nº 910/2014, de 23 de julio (Reglamento eIDAS), ofreciendo servicios de expedición de certificados cualificados. Sitio web: *https://www.logalty.com/*.

(19) Ejemplo: 54.247.116.13.

(20) Ejemplo: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.86 Safari/537.36.

(21) Ejemplo de SHA256: 196960b1921ae-7d3f8e596e44e922c9b1f7801a592a1a809b-67c97d91b14853c).

electrónicos contentivos de cualquier acto o hecho jurídico, incluyendo a cualquier tipo de manifestación de voluntad, generados de manera virtual.

2) Los documentos electrónicos debidamente certificados por un tercero de confianza que disponga de los mecanismos tecnológicos y los protocolos de seguridad idóneos para ello deben ser considerados documentos electrónicos firmados y pueden ser presentados en juicio como prueba documental en caso de que surja un litigio entre las partes a los fines de que el juez respectivo los valore mediante el correspondiente informe pericial informático.

3) Por último, y como conclusión final del presente estudio, se puede afirmar que, mediante el desarrollo y generalización de las transacciones comerciales electrónicas a través de la web, progresivamente se irá perfeccionando el régimen legal de los terceros de confianza con la finalidad de brindar seguridad jurídica a todas las partes involucradas en los contratos electrónicos certificados mediante dichas plataformas.

4) Igualmente, corresponderá a los órganos jurisdiccionales conocer y analizar cada caso en concreto, con base a las recientes normas legales dictadas en la materia (nos referimos al Decreto 182/2019 ya tratado), a los fines de crear los necesarios precedentes que sirvan para apuntalar la correspondiente validez jurídica de dichos documentos.

Nuevo paradigma contractual: los *smart contracts*

CARLOS D. MIRASSOU CANSECO (*) Y **ANDRÉS O. HADAD** (**)

I. Introducción

El mundo cambia constantemente. Si analizamos el último medio siglo veremos que cada 10 años —aproximadamente— el mundo vive una gran revolución tecnológica.

En la década del 70 aparecieron las placas madres, en los años 80 las pc, en los 90 internet, en los 2000 los *smartphones* y redes sociales. Claramente en esta década la revolución la protagonizan la inteligencia artificial y los datos. Parecería imposible y hasta contradictorio poder predecir cuál será la próxima revolución, así que nos enfocaremos en esta que parece haber llegado para quedarse.

La revolución digital, en general, y la de los datos, en particular (1), son dos de los mayores cambios de paradigma a nivel global que impactan fuerte y transversalmente en todas las actividades de nuestras sociedades.

Esto ha generado un crecimiento exponencial del volumen y del tipo de datos existentes, que son producidos a gran velocidad y en forma continua por personas —consciente e inconscientemente—, computadores, celulares, *tablets*, transacciones electrónicas y, principalmente, por el uso de Internet.

Así, muchas veces vemos que lo que era imposible ayer, probablemente mañana ya no lo sea. Hasta creemos que estamos en condiciones de afirmar que la persona que sostenga que algo no será posible tecnológicamente en algún momento, está equivocada. Está claro que no seremos nosotros sino la ciencia la que —tarde o temprano— terminará dándonos la razón.

Todo a su tiempo.

Hoy, resulta imprudente pedirle a la inteligencia artificial aquello que no puede ofrecer. Pero también resulta negligente no aprovechar las posibilidades que nos ofrece.

Varias de estas ofertas seguramente ya las conocemos porque, aunque cueste procesarlo y hasta a veces pase desapercibida, vivimos rodeados de inteligencia artificial: desde correctores ortográficos, diccionarios predictivos, reconocimiento facial y reconocimiento de la huella dactilar en nuestros móviles, hasta la predicción

(*) Abogado (UNL), prosecretario de la Presidencia de la Cámara de Apelaciones en lo Civil y Comercial de Santa Fe, maestrando en Argumentación Jurídica (UNL). Docente de nivel terciario.

(**) Abogado (UCSF), especialista en derecho notarial, registral e inmobiliario (UNL), maestrando en argumentación jurídica (UNL). Docente de nivel terciario y universitario.

(1) Para una mayor contextualización de la "revolución de los datos" ver Sosa Escudero, Walter, *Big Data*, 3ra Ed, Editorial Siglo Veintiuno, Buenos Aires, 2019; Schmarzo, Bill, *Big Data, el poder de los datos*, Ed. Anaya, Madrid, 2014; Marr, Bernard, *Big data en la práctica*, Ed. Teell.

de nuestros gustos personales que hacen las redes sociales a través del almacenamiento de nuestros patrones de búsqueda y visitas. ¿Quién no se sorprendió porque "mágicamente" el producto que buscábamos hace horas nos aparece como publicidad en todos los sitios?

Sí, es estremecedor el control ideológico que se tiene sobre nosotros, pero está ahí y es una realidad que lejos de acompañarnos ya nos ha sacado kilómetros de distancia. Y, si somos sinceros, tampoco podemos negar la comodidad que ello nos brinda.

Nos hemos acostumbrado a vivir sin saber cómo funcionan las cosas que utilizamos a diario. Es más, en este momento muy probablemente ni nosotros, ni los lectores de este artículo, entendamos plenamente cómo funciona la computadora que se utiliza diariamente para trabajar, menos todavía el celular que tenemos en nuestro bolsillo.

Sin embargo, la comodidad que nos ofrecen, como dijimos, es innegable. Cuando queremos saber algo, ya no es necesario recurrir a la biblioteca como años atrás; en pocos segundos abrimos algún buscador de internet y obtenemos millones de archivos que se vinculan con nuestro patrón de búsqueda.

Con todo ello no queremos ubicarnos en una posición hiper-entusiasta respecto de la inteligencia artificial, porque tal como lo ha dicho el juez Oliver W. Holmes —probablemente el jurista más influyente en toda la historia de los Estados Unidos— "la vida del Derecho no ha sido sólo lógica, sino también experiencia" (2) y a pesar de que esto muestre un paradigma muy contradictorio con lo que se intenta exponer, nos ayuda a abrir el campo de visión siempre que la entendamos como una herramienta para guiar y facilitar el desarrollo del derecho.

Es una herramienta innegablemente útil. A mayor cantidad de datos, más posibilidades de relacionarlos y por lo tanto de obtener mejores resultados.

Aunque haya poca doctrina y bibliografía nacional al respecto —sin desconocer el crecimiento exponencial en el último año—, es una necedad pensar que la utilización de la inteligencia artificial no está cambiando de manera paradigmática el pensar jurídico contemporáneo. Su uso ya traspasó la barrera de los buscadores de jurisprudencia, de legislación, de la implementación de los sistemas informáticos en juzgados, en la preselección de modelos de escritos, etc. Y si algo debemos tener claro, es que la inteligencia artificial llegó para quedarse.

II. Inteligencia artificial y algoritmos

En estos mismos instantes que nos encontramos escribiendo estas líneas, mejor dicho, en los últimos 60 segundos que acaban de pasar, en el mundo se mandaron cerca de cuatro mil quinientos millones de *mails*, más de medio millón de *tweets* y se realizaron alrededor de seis millones de búsquedas en la página de Google (3). Esto solo, implica que una cantidad inconmensurable de gigabytes sean procesados segundo a segundo en internet.

Está claro que nos encontramos frente a una revolución masiva de datos. Frente a ella se postula la necesidad de desarrollar herramientas que permitan analizarlos y procesarlos para identificar lo relevante. Estas herramientas, a las que preferimos llamar tecnologías, ya existen. Solo resta aprender a optimizar su uso. Y cuando hablamos de revolución, lo hacemos porque trasciende la simple idea de cantidad. No estamos hablando únicamente de muchos datos, sino de la generación de valor a partir de su procesamiento.

Sin lugar a dudas, la Inteligencia Artificial tiene un rol protagónico en este contexto. Un ejemplo con el que chocamos a diario pueden ser los datos que emitimos cuando hacemos valoraciones dentro de una escala —de una a cinco estrellas dependiendo si nos gustó más o menos una película—, entre otras técnicas, mediante las cuales las empresas que proveen servicios pretenden descubrir similitudes entre usuarios para que, por un lado, a cada uno se le ofrezca películas en función de sus preferencias, y por el otro, las plataformas —Netflix, Spotify, Facebook, etc.— valoren las preferen-

(2) Holmes, *The common law,* 1963.

(3) *Internet Live Stats*: *http://www.internetlivestats.com/one-second*, consultado el 9/8/19.

cias generalizadas de todos sus usuarios en miras de seguir cautivando nuevos usuarios.

En síntesis, actualmente la Inteligencia Artificial es la tecnología clave de la sociedad de la información y del conocimiento, lo que supone la utilización de diferentes técnicas para resolver problemas, maximizar objetivos y optimizar el procesamiento de información.

Estas y otras cuestiones desencadenadas en el marco de la llamada "Cuarta Revolución Industrial" —en palabras del Foro Económico Mundial— (4) nos sitúan en un escenario de transformación profunda en lo que hacemos y en lo que somos.

Este cambio monumental, en esencia, responde a dos grandes fenómenos que se entrelazan. El primero es la mutación radical de las nociones de espacio y tiempo a partir del uso masivo de nuevas tecnologías de la información y de la comunicación (TIC) y el segundo son las nuevas formas de procesar datos e información, en muchas actividades que antes solo podían ser realizadas por nuestros cerebros (5).

Introducidos en este nuevo paradigma de inteligencia artificial, hablaremos de una de las tantas formas que tiene de relacionarse con el Derecho. Para ello es óbice necesario hacer referencia a ciertas aplicaciones que en algunos países han revolucionado —y en otros lo revolucionarán— el mundo de los servicios financieros desde hace un par de años y que ahora están incursionando en el mundo de los servicios jurídicos con la capacidad de cambiar radicalmente la forma en que concebimos la ejecutabilidad de las obligaciones dentro de acuerdo contractual.

Nos estamos refiriendo a la tecnología *blockchain* y más específicamente a los denominados contratos inteligentes (*smarts contracts*, en inglés).

Por supuesto, no pretendemos explicar con todo el nivel de detalle estos conceptos, sino más bien intentaremos dar una introducción a los mismos, teniendo en cuenta que por su novedosa aparición se encuentran en constante perfeccionamiento.

III. Su clave: los algoritmos

La inteligencia artificial en particular procesa esos datos a través de su clave: los algoritmos.

"Algoritmo" es una palabra que debemos conocer si queremos aprender el funcionamiento interno de los *Smart Contracts*. Se puede decir que es un conjunto preciso de instrucciones o reglas, o también una serie metódica de pasos que puede utilizarse para hacer cálculos, resolver problemas y tomar decisiones.

En otras palabras, podemos decir que es un esquema ejecutivo donde se almacenan todas las opciones de decisión en función de los datos que se vayan conociendo.

A estos esquemas se los puede representar en "diagramas de flujo" que son básicamente la descripción pormenorizada de las opciones que representa el esquema, tal como si fuera un campo neuronal, en donde todo está conectado.

A continuación, un ejemplo improvisado al solo efecto de clarificar el concepto de "diagrama de flujo".

Compramos un pasaje de avión (contrato) entre cuyas cláusulas encontramos las siguientes:

Opción 1: el vuelo despega a horario

1.a.: me dan el almuerzo; 1.a.a.: soy celíaco y no tienen menú para mí;

1.b.: no me dan el almuerzo/merienda/cena pactado;

1.c.: no me dan la almohada y manta;

(4) Para un mayor desarrollo de este concepto, ver Corvalán, Juan Gustavo, "Hacia una óptima administración digital e inteligente", La Ley, 19/10/2017, cita online: AR/DOC/2784/2017; Gil, Gabriela F., "La inteligencia predictiva como herramienta de eficacia en la gestión judicial", SJA 21/11/2018, 21/11/2018, 35, cita online: AP/DOC/903/2018; Díaz, Viviana L., "Revolución industrial 4.0. ¿Destrucción o nacimiento de la fuerza laboral?", RDLSS 2017-9, 17/05/2017, 875, cita online: AP/DOC/284/2017.

(5) Corvalán, Juan G., "PROMETEA. Inteligencia Artificial para transformar organizaciones públicas", en *www.dpicuantico.com*, Diario Administrativo Nro. 228 - 26.02.2019.

1.d.: no se reclina mi asiento;

1.a.a.; 1.a.b. = será depositado el 10% del valor del pasaje automáticamente en la cuenta de la tarjeta con la que pagué el vuelo o, si lo compré con dinero en efectivo, en la cuenta que tuve que denunciar como garantía del SC.

1.b = será depositado el 15% del valor del pasaje automáticamente...

1.c.= será depositado el 5% del valor del pasaje automáticamente...

1.d.= será depositado el 10% del valor del pasaje automáticamente...

Opción 2: el vuelo se retrasa

2.a.: se retrasa menos de 19 minutos;

2.b.: se retrasa entre 20 y 60 minutos;

2.c: se retrasa entre 61 y 120 minutos;

2.d.: se retrasa entre 121 minutos y 23 hs;

2.e: se retrasa 24 hs o más.

2.a = no corresponde indemnización.

2.b= será depositado el 15% del valor del pasaje automáticamente en la cuenta de la tarjeta con la que pagué el vuelo o si lo compré con dinero en efectivo en la cuenta que tuve que denunciar como garantía del SC.

2.c= será depositado el 30% del valor del pasaje automáticamente...

2.d= será depositado el 45% del valor del pasaje automáticamente...

2.e= por cada día de retraso —y con un máximo de 2— se depositará el 50% del valor del pasaje...

2.c ; 2.d ; 2.e = si implica la pérdida de otro pasaje se adiciona automáticamente a la indemnización mencionada el costo íntegro del pasaje perdido + US$ 150 en concepto de compensatorios.

2.d; 2.e = se adiciona a las indemnizaciones que correspondan la reserva y pago automático de una noche de hotel + cena/almuerzo en lugar a determinar por la ubicación geográfica del pasajero al momento de la pérdida del vuelo, todo lo cual se le informará al consumidor en los 15 minutos próximos a los 121 minutos.

Y así podríamos seguir inventando infinitas eventualidades con sus correspondientes consecuencias.

Una opción sería pensar que todo esto se realizaría a través del intercambio automático de datos generado entre el S.C. y la torre de control que oficiaría para este supuesto como "oráculo" (6).

Para una sistematización y cabal comprensión de estas estructuras, pasemos a lo que hoy nos convoca.

IV. La cadena de bloques o *blockchain*

Si hablamos de paradigma digital, revolución de los datos, *big data*, *bitcoins*, aprendizaje automático o *machine learning*, inteligencia artificial, internet de las cosas o IoT, etc., es imposible no referirnos a las cadenas de bloques (*blockchain*, en inglés).

Este concepto está posibilitando a pasos agigantados hacer realidad todo este tipo de avances tecnológicos, y aunque pueda resultar tedioso, es necesaria su comprensión para entender verdaderamente cómo funcionan los contratos inteligentes.

Muchas de las instituciones financieras más prestigiosas del mundo están realizando una investigación de cadena de bloques en estos momentos. En 2017 se estima que un 20% de los bancos la utilizaron (7) cuadriplicándose ese porcentaje en las proyecciones esperadas

(6) Para una mejor comprensión de la función y concepto del "oráculo" ver Slobodník, J. en "How Oracles connect Smart Contracts to the real world", disponible en: *https://medium.com/bethereum/how-oracles-connect-smart-contracts-to-the-real-world-a56d3ed6a507*; también en "¿Qué es el oráculo y como se vincula con los SC? disponible en *https://www.miethereum.com/smart-contracts/*.

(7) Gupta, Vinay. "A Brief History of Blockchain", *Harvard Business Review*,28 de febrero de 2018, *https://hbr.org/2017/02/a-brief-history-of-blockchain*.

para el año que viene (8). MasterCard, Visa, BBVA, Banco Santander, IBM, son tan solo algunos ejemplos de empresas que utilizan esta tecnología.

Se trata de una base de datos distribuidos, automatizada, descentralizada, inalterable (9) —por lo menos hasta ahora—, en la cual se registran operaciones de intercambio de información entre dos o más partes. En pocas palabras, también podríamos definir esta tecnología como un registro único, consensuado y distribuido en varios nodos de una red (10).

Decimos "descentralizada" porque está replicada en todos los ordenadores de los usuarios, es decir, que los datos se encuentran almacenados en múltiples equipos que tienen acceso independiente a toda la información, pero de forma encriptada.

A su vez, la única forma en que una transacción sea válida es que aparezca escrita exactamente igual y al mismo tiempo en todos los libros que tengan todos los participantes de la red. Lo mismo sucede con cada nuevo bloque de información, es necesario que se lo dote de la autenticidad del viejo bloque, para permitirle formar parte de la cadena. Todos los bloques que conforman la cadena utilizan una contraseña numérica llamada *hash*, tomada del bloque anterior. A esta transacción se le da un número único y se la agrega al listado de todas las transacciones realizadas previamente, formando así una cadena de bloques (de ahí el nombre *blockchain*).

Otro ejemplo para clarificar. Pensemos que el *blockchain* es un libro contable donde se dejan asentadas operaciones financieras, solo que a este libro no lo tiene un único propietario, sino que es replicado y custodiado por diferentes personas en tiempo real. De ahí viene el otro nombre de "contabilidad distribuida" con el que también se suele llamar a esta cadena de bloques.

Por supuesto, esto ocurre en cuestión de segundos, toda vez que se realiza mediante múltiples computadores con características superiores a las normales.

De hecho, la principal característica radica en que la seguridad de la información es, casi, a prueba de errores, toda vez que todos los "libros" deben contener exactamente la misma información para que una transacción sea válida.

Así las cosas, si alguien quisiera alterar la integridad de la cadena, la arquitectura de funcionamiento de las *blockchains* hace que la falsificación de los datos sea muy difícil. Por su encadenamiento de datos y sus claves criptográficas, para que la cadena de bloques pueda verse fraguada se requiere que los servidores se pongan de acuerdo en la defraudación y —sin conocerse entre sí— lo hagan todos al mismo tiempo, lo cual resulta inimaginable.

El gran salto que implicó esta tecnología es haber logrado migrar de un Internet en el que solo se intercambiaba información a uno en el cual lo que intercambiaremos será "valor".

Por lo tanto y en relación con los contratos en particular, en *blockchain* se pueden registrar las operaciones, fechas, cantidades, participantes, y además puede contener no solo información sino cualquier cosa que tenga valor, como dinero, acciones en bolsa, bonos e incluso votos de elecciones.

V. Paradigma contractual

Para introducirnos de lleno en el tema que hoy nos convoca, nos gustaría apuntar unas breves reseñas respecto a esta nueva realidad negocial que nos envuelve.

El giro rotundo operado en las formas en que hoy llevamos adelante distintos tipos de nego-

(8) "El 80% de las entidades financieras espera adoptar el «blockchain» para 2020" en *https://www.abc.es/tecnologia/redes/abci-80-por-ciento-entidades-financieras-espera-adoptar-blockchain-para-2020-201707050944_noticia.html*.

(9) El fundamento de la inalterabilidad es que, a los fines de generar un bloque fraudulento, debería modificar todos los bloques anteriores donde se guardaron información, y se fueron generando códigos únicos que nos permiten corroborar la autenticidad.

(10) V. Pastorino, Cecilia, "Blockchain: qué es, cómo funciona y cómo se está usando en el mercado" de fecha 04/09/18, disponible en *https://www.welivesecurity.com/la-es/2018/09/04/blockchain-que-es-como-funciona-y-como-se-esta-usando-en-el-mercado/*.

cios es indiscutible. Lo propio sucede con una de las principales herramientas para llevar estos negocios adelante: los contratos.

Así, en un primer momento, la figura contractual del código velezano –vigente hasta hace unos pocos años— respondía al acuerdo de voluntades celebrado de modo instantáneo, discontinuo, entre iguales y de cambio. Tipificaba el llamado "modelo clásico" de contrato.

Al respecto y como antecedente de esta concepción del contrato como decisión futura, resulta muy interesante la teoría del norteamericano Ian Mcneil de los contratos relacionales.

Según este autor, el contrato clásico, paradigma de la ideología liberal, se identifica como "contrato discontinuo", porque contiene en el presente de su celebración todos los comportamientos a ser realizados en el futuro. Este contrato sería el típico instrumento de intercambio.

Así, corresponderían a este modelo los principios de autonomía de la voluntad, de determinación en cuanto al objeto, de inmodificabilidad del contrato, etc. Sin embargo, Mcneil plantea que en nuestra realidad contemporánea, los contratos son mucho más complejos que los previstos por este modelo cerrado, y las soluciones jurídicas que da el modelo clásico del contrato por lo tanto no resultarían eficientes (11).

Entre las características que distinguirían a estos contratos que harían ineficaz el modelo clásico, estaría que los llamados "contratos relacionales" tendrían una larga duración, y, sobre todo, la presencia de cláusulas abiertas que les dan a las partes flexibilidad para alcanzar futuros acuerdos. Estas cláusulas abiertas serían importantes cuando se planean negocios complejos de largo plazo, o en economías tan cambiantes como la nuestra. Se pueden encontrar cláusulas de ajustes de precios, o cláusulas de distribución de riesgos, entre otros ejemplos.

De ese modo, se buscan mecanismos que faciliten el acuerdo de voluntades entre las partes a través de todo el proceso contractual, en vez de limitar dicho acuerdo al momento del perfeccionamiento formal del contrato, disminuyendo la incidencia de comportamientos oportunistas (12).

Hoy, el concepto estático del contrato creemos que ha sido superado. Se lo piensa de una manera mucho más dinámica, como un "proceso" que liga a sus partícipes y se dirige a una finalidad específica –el cumplimiento—, que atraviesa diversas fases en su desarrollo, comenzando desde las tratativas, pasando por la conclusión y ejecución, y hasta incluso pudiendo alcanzar el período poscontractual.

De esta manera vemos cómo el contrato es una figura con vida propia que lejos de nacer y morir en un mismo momento, hoy tiende a prolongarse y extenderse, situación que conlleva a que pueda estar sujeto a mayores eventualidades.

VI. Contratos inteligentes o *smarts contracts*

A pesar de que su nombre da indicios acerca de qué se tratan, para entender qué son realmente y cómo funcionan es necesario realizar una explicación más profunda y técnica, la cual intentaremos desarrollar a continuación, debido a que nuestro derecho todavía no los contempla expresamente ni contamos con precedentes judiciales que ayuden al respecto.

Los contratos inteligentes se pueden definir como programas informáticos que facilitan, aseguran, hacen cumplir y ejecutan acuerdos registrados entre dos o más partes (personas físicas o jurídicas). Son algoritmos que operan con la característica principal de no poder ser controlados por ninguna de las partes y de ser autoejecutables, es decir, su ejecución se encuentra automatizada (13).

(11) Ver Macneil, Ian, "Contracts: adjustment of long-term economic relations under classical, neoclassical, and relational contract law", Nw. UL Rev., 1977,72, Chicago, p. 854.

(12) Ver Macneil, Ian, "Relational contract theory: challenges and queries", *Revista de abogados de la Universidad de Northwester*, año 1999, p. 844.

(13) En este sentido es de gran ayuda la analogía de entender que el *code is law*, es decir que "el código es la ley", de manera que la función del "programador" se asimilaría a la del "legislador".

VII. Su funcionamiento

El tema no es tan complejo como aparenta. A modo de aproximación intentaremos brindar una breve explicación.

El programa funciona con líneas de código de programación de las conocidas como *if-then* o *if then else*. Esta función resulta útil para crear una variedad de elementos calculados de distintas maneras para filtrar, agrupar y volver a rotular, excluir o segmentar los resultados. Si se usa *if then else*, se tiene que proporcionar un elemento o condición que sirva para probar y ciertos valores que sirvan para reflejar los resultados dependiendo si la expresión se cumple o no.

Esta expresión puede definirse de dos maneras (14):

- IF (condición booleana, es decir, que solo admite dos respuestas posibles) THEN (valor verdadero) ELSE (valor falso) ENDIF: el resultado devuelto dependerá de si la condición se cumple o no.

- IF (condición booleana) THEN (valor verdadero) ENDIF: el resultado devuelto siempre será el resultado verdadero. Si eliminamos el "ELSE" los resultados se filtran. Si la expresión condicional no se cumple, el resultado estará vacío.

La verificación de que la condición preestablecida no se realizará también producirá consecuencias. En efecto, la no concurrencia de las condiciones prefijadas se suele incluir en el término *else*, de manera que desencadenará una acción distinta; por ejemplo, la devolución del dinero anticipado depositado en una cuenta.

Es como si fuera un sistema de respuesta predeterminadas y automáticas, si ocurre "A" entonces sucede "Y", pero la diferencia radica en que se realiza de una manera que interactúa con activos reales. Es decir, dos partes o más —probablemente a través de sus abogados— se ponen de acuerdo en las cláusulas que los obligarán, arman el programa en base a ello y lo suben al sistema *blockchain* —probablemente con la ayuda de un programador—; a partir de ahí, el contrato se encarga de ir analizando las condiciones, ejecutando un algoritmo u otro, dependiendo de lo que vaya aconteciendo.

Si bien normalmente también se componen de una interfaz de usuario y a veces emulan la lógica de las cláusulas contractuales, cuando se dispara una condición preprogramada, no sujeta a ningún tipo de valoración humana, el contrato "inteligente" ejecuta la cláusula contractual correspondiente de manera automática.

Un factor interesante se presenta en la búsqueda de información externa.

Aquí aparece el concepto de oráculo, antes mencionado. Es la herramienta informática que le permite al *smart contract* autoejecutarse al verificar previamente cierta información —por ejemplo, precios oficiales de divisas, cotización de acciones, información de la torre de control sobre el despegue de los vuelos en el ejemplo arriba mencionado, resultado de algún partido deportivo en donde se hayan realizado apuestas, etc.—. Vemos un claro inconveniente en esta "tercerización" de la información porque para ello siempre habrá que recurrir a una fuente (tercero) externa y por lo tanto un intermediario por fuera de la *blockchain*, perdiendo así parte de la confianza tan publicitada. Claramente que esta es una cuestión que pulir y de ello se han hecho eco algunas empresas (15).

VIII. Su principal característica

Estos tipos de contratos fueron creados con el objetivo de brindar una seguridad superior al contrato tradicional y reducir costos de transacción asociados a la contratación, como los relacionados con la ejecución por incumplimiento.

Esa característica distintiva llamada "autoejecución" es la que lo dota de ciertas particularidades que lo diferencian cabalmente de los contratos tradicionales.

(14) Cfr. Puterbaugh, *The future of contracts: automation, blockchain, and smart contracts*, número 34, diciembre 2016, p. 50.

(15) Por ejemplo "Oraclize" de la firma Provable (*http://provable.xyz*) que ya está implementando un sistema de comparación de información de distintas fuentes a los efectos de arrojar resultados sumamente confiables y válidos.

Las partes acuerdan que el contrato se vaya ejecutando directamente según el cumplimiento o no de lo pactado y sin necesidad de terceros.

En este sentido, no debemos olvidar que nos encontramos ante un algoritmo o "código informático" que existe en una cadena de bloques compartida, con la característica de no poder ser modificada por las partes.

Así, la posibilidad de ejecutar las obligaciones adquiridas en un acuerdo contractual sin la necesidad de recurrir por vía jurisdiccional a que un juez obligue al deudor moroso al cumplimiento de lo contratado seguramente cambiará de manera radical la forma en que concebimos la ejecutabilidad de las obligaciones en los acuerdos contractuales.

En otras palabras, se lograría superar la barrera impuesta de la monopolización del Derecho por parte del Estado permitiendo una administración de justicia más efectiva, especialmente en relación con la velocidad de la ejecutabilidad inmediata del contrato incumplido, gracias a que los ciudadanos se han autorregulado y confiado en un tercero descentralizado para asegurar el cumplimiento de los acuerdos a los que han llegado.

En conclusión, los *smart contracts* y, en general, las tecnologías que habilitan la descentralización de los medios de producción y/o del poder de coerción, proveen su mayor beneficio al descongestionar las funciones que tradicionalmente solo estaban permitidas al Estado; sin duda alguna, algo que nos vendría muy bien en nuestro país.

IX. Ventajas y desventajas

Como todo, cuenta con sus ventajas y desventajas. No obstante, hay que señalar que al estar en permanente desarrollo se continúa trabajando para optimizar su funcionamiento al máximo.

Como ya se dijo, todo este tipo de tecnología con capacidades de autogestionarse nos habilita a una descentralización, especialmente a la hora de solucionar conflictos que surgen de los incumplimientos —totales o parciales— de negocios. Esa delegación históricamente realizada al estado, bajo la fuerza de la función jurisdiccional, es "tercerizada", ante terceros privados, que tratan de brindarnos todas las herramientas necesarias para protegernos como consumidores, y vendedores.

De esta manera, los *smart contracts* lograrían superar la barrera impuesta de la monopolización del Derecho ahorrando tiempo y dinero, ya que no se deberá pagar escribanos, gastos de procesos judiciales y todo lo vinculado a costas judiciales, etcétera.

Otra ventaja que trae aparejada es que, al ser un contrato digital que funciona en la *Blockchain*, es prácticamente imposible de modificar o destruir, lo cual traduce su alto grado de seguridad.

Esta inalterabilidad de la información allí contenida es a prueba de errores, toda vez que todos los "libros" deben contener exactamente la misma información para que una transacción sea válida. De esta manera si alguien quisiera alterar la integridad de la cadena, deberá hacerlo en todos los equipos de forma simultánea.

Algunos o todos los términos de un acuerdo propuesto en lenguaje natural podrían ser traducido al código o codificado en lenguaje de scripting directamente.

El código podría ser ventajoso al redactar ciertas cláusulas operacionales (por ejemplo, cláusulas de pago) en los acuerdos legales; y si bien es cierto que es más limitado que el lenguaje natural, no es menos cierto que proporciona menos espacio para la ambigüedad, por lo que podría decirse que mientras que el código de computadora está sujeto al error humano, está mucho menos sujeto a incertidumbre.

Desventajas

Por otro lado, y como todo en realidad, este tipo de programas también tienen ciertas desventajas, o más bien obstáculos que superar.

Como se sabe, la automatización de este tipo de procesos, y la industria en general, vienen acompañado de una problemática vinculada al desempleo, o podemos definirlo en mejores términos, y al decir de los autores Cevasco y Corvalán "una nueva configuración en la divi-

sión de tareas" (16), ya que será inevitable que en esta oleadas tecnológicas deje afuera ciertas tareas tradicionales realizadas por personas, y dependerá también del estado el aprovechar la potencialidad de su población para orientarla laboralmente a todo ese sector que todavía no ha sido explotado (como puede ser, la programación).

También encontramos ciertas desventajas cuando miramos las tecnologías de las que se vale, esto es, IoT y *blockchain*. Mientras que el IoT puede permitir una verdadera vinculación con activos reales, lo cierto es que aún le queda un largo camino en seguridad. Los dispositivos IoT son fácilmente hackeables, algo que grandes empresas ya se han unido para solventar (17).

En este sentido, en segundo lugar, debe decirse que surgen contingencias novedosas, como por ejemplo que —en tanto las transacciones son irreversibles— un error o un contrato inteligente mal programado pase a bloquear eternamente los fondos recibidos (18). Aquí cabe mencionar que también existen limitaciones en su "redacción", las cuales lógicamente se traducirán en una incompleta determinación del código, el cual nunca podrá capturar el dinamismo del mundo real, siendo inimaginable que algún contrato, del tipo que sea, refleje la totalidad de las eventualidades que pueden suceder.

Podemos sumar que a pesar de que la inmutabilidad del contrato sea un punto a favor en cuanto a seguridad, ello puede convertirse en una desventaja ante distintas eventualidades, ya que en muchas ocasiones puede haber agentes externos que puedan alterar el acuerdo por alguna razón, por ejemplo, casos fortuitos o de fuerza mayor.

A pesar de que se está trabajando en una *blockchain* con la posibilidad de ser modificada, esto quitaría el aspecto más beneficioso de esta, ya que al permitir dicha acción podría facilitar los ataques informáticos para alterarla. Sin embargo, dependiendo de cómo sea implementado el sistema, creemos que podría funcionar. Por el momento esto no parece algo posible.

Por último, también podemos apuntar el gran obstáculo que supone crearlos. Los *smart contracts* tienen un grave problema con respecto a su elaboración, ya que es necesario contar con formación sobre informática para poder programarlos. Ello torna necesario recurrir a personas que contengan dichos conocimientos y, además, también sepan sobre leyes.

Un cambio más que interesante para las clásicas carreras de abogacía que apoyan su currícula en el derecho decimonónico.

No obstante, muchos proyectos como *Ethereum* han dado la posibilidad de crear los contratos con mayor facilidad y a través de una interfaz más amigable. Aunque a la vez cabe señalar nuevamente que esta tecnología cuenta con pocos años en la práctica, por lo que posiblemente en un futuro crear un contrato inteligente sea tan fácil como hacer un blog en la actualidad.

X. Desafíos jurídicos suscitados

Claramente, nos encontramos ante un gran desafío en lo que refiere a su encuadre jurídico.

Los *smart contracts* plantean varias cuestiones desde la óptica legal. Nuestro derecho no los contempla, ni contamos todavía con precedentes judiciales que ayuden demasiado al respecto. Pero la normativa general de con-

(16) Cevasco, Luis J. y Corvalán, Juan G, "¿Desempleo tecnológico? el impacto de la inteligencia artificial y la robótica en el trabajo", en La Ley 11/07/2018, 1.

(17) En este contexto, se ha dicho que dos de los principales motivos por los que los *smart contracts* se han aplicado poco hasta ahora son: de una parte, la dificultad que presentan para controlar activos reales –el código informático no tiene control «físico» sobre ellos– de modo que no "asegura" la "ejecución" del contrato inteligente; y, de otra, la inexistencia de un ordenador "neutral" en el que depositar la confianza de la ejecución; este último aspecto, lógicamente, puede ser suplido por acuerdo de las partes. A lo anterior, también cabe añadir la numerosa y estricta regulación de control para efectuar transferencias patrimoniales electrónicas (cfr. Morell Ramos, "Cómo crear un *smart contract* mediante términos y condiciones. *Smart contracts*: teoría, práctica y cuestiones legales", 21 de septiembre de 2016, *https://goo.gl/2UnwZY*).

(18) Ver Mora, Santiago J., "La tecnología blockchain. Contratos inteligentes, ofertas iniciales de monedas y demás casos de uso", La Ley 1/4/2019, 1; cita online: AR/DOC/537/2019.

tratos sí que aporta criterios para verificar si un *smart contract* puede tener validez jurídica y capacidad de ser legalmente exigible.

Nuestro sistema legal reconoce la autonomía de las partes para alcanzar acuerdos legalmente exigibles y contratar libremente en los términos que consideren, siempre que se cumplan las exigencias básicas del derecho de contratos (19), tanto en que su contenido sea un objeto lícito (20) como en el modo de formalizarlos (21).

Algo parecido podemos ver con la implementación de las criptomonedas. Actualmente existen países que ya implementaron el *bitcoin* como medio de pago legal. Un ejemplo emblemático es Japón. El interrogante puede suscitarse entonces para el caso de una empresa argentina que negocie con una empresa japonesa cuando el lugar de cumplimiento de las obligaciones sea en Japón y que, conforme a nuestro art. 2652 del Cód. Civ. y Com., el contrato deba regirse "por las leyes y usos del país del lugar de cumplimiento". ¿Qué pasa entonces si la empresa argentina se resiste a aceptar el pago en *bitcoins*? En el caso de aceptar el pago en criptomonedas, ¿cómo se tributa sobre ello? ¿cómo un bien, una cosa, un activo financiero, una moneda? (22).

Volviendo a los *smart contracts*, al estar basados en *blockchains* también suponen retos para su eficacia legal.

La *Blockchain* —como sistema de registro— cumple perfectamente con el concepto de "documentos digitales con firmas electrónicas", incorporados en nuestro derecho por los arts. 5º y 6º de la ley 25.506 de Firma Digital. También resulta evidente que si bien estos sistemas parecieran tener una aplicación inmediata para las personas privadas que quieran registrar distintos aspectos de las relaciones contractuales entre ellos, la situación se torna un poco más compleja en lo que hace a los registros públicos (23).

Incluso la ley 27446, en su art. 10, consagra una presunción *iuris tantum:* "Cuando un documento electrónico sea firmado por un certificado de aplicación, se presumirá, salvo prueba en contrario, que el documento firmado proviene de la persona titular del certificado".

Por otro lado, se ha dicho que a los contratos inteligentes no les importa si la ejecución puede resultar injusta ni tampoco importan los hechos o los comportamientos sociales efectivos en torno a ellos. En el mismo sentido, dado que una vez que se activan los contratos inteligentes las partes pierden control sobre su ejecución y no se pueden dejar de cumplir, deberá analizarse cómo se conjuga ello con el régimen de vicisitudes de los contratos, entre otras cuestiones (24).

En cuanto a la voluntad de las partes intervinientes, un *smart contract* formalizado exclusivamente en código informático y registrado en la cadena de bloques puede suscitar dudas en cuanto a la validez del consentimiento contractual en contrataciones masivas, cuando no sea posible acreditar que todas las partes intervinientes en la formalización son expertas en ese lenguaje de programación, o que aun no siéndolo se ha formulado también en lenguaje natural o que ha sido efectivamente comprendido (25).

Caso aparte se configurará cuando el contrato refleje operaciones o relaciones de consumo. Así, en muchos contratos inteligentes una de las

(19) Ver arts. 957, ss. y cc. del Cód. Civ. y Com.

(20) Asimismo que no contravenga normas legales imperativas, existencia de consentimiento válido de las partes, y obedecer a una causa lícita —no cabría dar eficacia jurídica, por ejemplo, a un smart contract que tenga por objeto una transferencia de activos de tráfico prohibido—.

(21) Ver arts. 284, 1019 y 1020 del Cód. Civ. y Com.

(22) Branciforte, Fernando, "Las nuevas tecnologías y el Derecho", La Ley 22/07/2019, 1, cita online AR/DOC/2232/2019.

(23) Mora, Santiago J., "La tecnología blockchain. Contratos inteligentes, ofertas iniciales de monedas y demás casos de uso", La Ley 01/04/2019, cita online: AR/DOC/537/2019.

(24) Ver Morell Ramos, Jorge, "*Smart contracts:* teoría, práctica y cuestiones legales", publicado el 21/09/2016 en *www.terminosycondiciones.es*, citado por Mora, Santiago J., "La tecnología blockchain. Contratos inteligentes, ofertas iniciales de monedas y demás casos de uso", La Ley 01/04/2019, 1; cita online: AR/DOC/537/2019.

(25) Conf. arts. 285 a 288 Cód. Civ. y Com.

partes será predisponente, siendo múltiples las ocasiones en las que la otra parte ostentará —además— la condición de consumidor o usuario. En estos casos, a la habitual posición de desventaja que se hace patente en los contratos de adhesión o de consumo tradicionales se suma el usual desconocimiento de las tecnologías sobre las que se construye y las particularidades de la ejecución automática. De esta manera, existirá en el caso un especial deber de información (26), base fundante del derecho al consumidor.

Asimismo, pueden presentar conflictos los *smart contracts* que no se concluyan entre personas físicas o jurídicas, sino directamente entre computadoras o entre cosas —PC, heladera, dispositivos móviles, aire acondicionados, etc.— conectadas a través del IoT o "internet de las cosas". Un ejemplo de esto: una heladera "comprueba" la falta de manteca y "emite" una "orden de compra" al supermercado que a su vez remite la manteca al domicilio del propietario de la heladera (27).

Obviamente la ley únicamente admite la contratación entre personas, así que a efectos legales siempre habrá que buscar quién es la persona física o jurídica bajo cuyo control actúa el dispositivo o agente, y a quien se atribuirán las obligaciones y responsabilidades pertinentes.

Y, aunque uno de los elementos diferenciales que se asocia a las tecnologías *blockchain* es la fiabilidad de transacciones entre partes que no se conocen en un entorno sin intermediario centralizado, habrá que ver desde el punto de vista probatorio si, en caso de litigio, los tribunales consideran que se han generado evidencias suficientemente sólidas de la identidad de las partes, del consentimiento sobre el contenido de lo acordado, y de la fecha y hora; aunque estas cuestiones serían menores en los casos de *smart contracts* utilizados en *blockchains* privadas.

Está claro, que al asesorar sobre la utilización de *smart contracts*, se deberá trabajar mano a mano con ingenieros y expertos en programación de *software* para poder trasladar los esquemas legales a algoritmos que den lugar a estructuras transaccionales autoejecutables y que a la vez resulten legalmente exigibles.

Sin lugar a duda, todo ello hace de esta novedosa figura un desafío apasionante, no solamente para los profesionales sino, primordialmente para las Universidades que deberán revisar el contenido de la currícula, en particular la manera de enseñar los contratos y las obligaciones, para adecuarla a las exigencias actuales de regulación de estas novedosas formas negociales; como así también para el Poder Judicial que deberá enfrentarse con esta realidad al tener que interpretar el contenido y alcance de este tipo de institutos.

XI. Ejemplos

Quizá algunas de estas ejemplificaciones puedan resultar un tanto simplistas en relación con el potencial que realmente ostentan estas herramientas tecnológicas. Sus implicaciones son inimaginables especialmente cuando se combinan con otras tecnologías como Internet de las Cosas.

Uber Technologies Inc. es una empresa internacional que proporciona a sus clientes vehículos de transporte con conductor (VTC), a través de su *software* de aplicación móvil (App), que conecta los pasajeros con los conductores de vehículos registrados, los cuales ofrecen un servicio de transporte a particulares. Esta aplicación informática convierte el contrato de transporte de personas en un *smart contract* o contrato inteligente, que en función de un programa aportado por un tercero permite concertar y ejecutar acuerdos entre el chofer o transportista y el cliente o transportado, previendo la gran mayoría de las circunstancias a través de las cuales se opera en la materia (28).

En el ámbito del derecho del trabajo pensemos, por ejemplo, en el contrato de temporada, contenido en una aplicación informática donde todo está previsto, garantizándole al trabajador el

(26) Consagrado en el art. 4°, de la ley 24.240.

(27) Granero, Horacio R., "Los contratos inteligentes y la tecnología 'blockchain'", en *El Dial* de fecha 07/03/2018.

(28) De Diego, Julián A., "Smart contracts o contratos inteligentes. La influencia de Uber a través de aplicaciones informáticas", La Ley 1/10/2018, 1 - LA LEY 2018-E, 1283; cita online: AR/DOC/1651/2018.

cobro de sus salarios y sus ajustes, las condiciones de trabajo, generando automáticamente la convocatoria a cada temporada, y estableciendo los mecanismos de extinción, asegurando las indemnizaciones que pudieren corresponder.

En este sentido, los fideicomisos podrían también ser reemplazados por contratos inteligentes basados en *blockchain*: si tres personas, por ejemplo, pautan el depósito de determinado monto de dinero en un plazo estipulado para comprar un bien, y solo dos de ellas cumplen lo pautado en tiempo y forma, la cadena de bloques permitiría fácilmente que el contrato se termine y que el monto depositado sea devuelto a los respectivos inversores de una manera rápida y sencilla (arts. 1666 y ss. del Cód. Civ. y Com.).

Otro ejemplo muy vinculado al sector *freelance* del mundo del diseño y la programación, lo encontramos en las plataformas que funcionan como las clásicas "consultoras", que reciben currículum vitae de postulantes de trabajos, y los vincula con personas de cualquier lado del mundo, que estén necesitando un perfil con dichas aptitudes. Si bien la entrevista entre el prestador del servicio, y la persona que lo necesita es fundamental para que el trabajo se realice en forma, toda la relación se plasma por medio de la página que intermedia, donde cada parte pone sus condiciones, plazos para cumplimiento, y se realiza un control de forma digital de que las partes vayan acreditando los requisitos exigidos, luego de lo cual se procede a la liberación del dinero pactado en retribución de los servicios prestados.

Para finalizar con los ejemplos queremos mencionar la prueba que actualmente está realizando la empresa japonesa Toyota, utilizando este tipo de contratos para la venta financiada de vehículos. De modo tal que mes a mes el *smart contract* verificará el pago de la cuota y ante la falta de ingreso del dinero en el plazo pactado, inmediatamente, en tiempo real, enviará una orden satelital al vehículo objeto del contrato produciendo su inmediata detención sin posibilidad de utilizarse hasta tanto se salde la mora en el pago de la cuota (29).

(29) Branciforte, Fernando, "Las nuevas tecnologías y el Derecho", La Ley 22/7/2019, 1, cita online AR/DOC/2232/2019.

XII. Conclusiones finales

Claramente que con el presente trabajo no se ha pretendido ilustrar acerca de los pormenores de esta novedosa figura, pero si, al menos, introducir al público jurídico en un tema que sin dudas ha llegado para quedarse.

Desde finales de siglo XX asistimos a una nueva etapa signada por el desarrollo de formas de producción de bienes y servicios habilitadas por nuevas tecnologías que irrumpen y se difunden rápidamente, posibilitando una competencia y acceso a los mercados mucho mayor, derrumbando así ventajas competitivas.

La nueva realidad representada por tecnologías innovadoras nos enfrenta a cambios de paradigmas que sustituyen parte del trabajo del ser humano por algoritmos más precisos y menos conflictivos, permitiendo una centralización decisoria que posiblemente reemplazará la dispersión de centro de decisión que traducen y ejecutan la infinita cantidad de interrelaciones que se producen en la sociedad.

Este cambio, a pesar del temor y rechazo que seguramente en muchos genera, no se va a detener. Creemos que la clave se encuentra en cómo posicionarnos desde el derecho frente a semejante avance tecnológico.

Nos encontramos así frente a un mundo jurídico que, por un lado, se encuentra permeado indefectiblemente por este fenómeno y, por el otro, está signado por tendencias conservadoras en donde la primera reacción por lo general consiste en alertar acerca de los peligros de la innovación en vez de por descubrir sus ventajas (30).

Esta primera reacción que es aislarse, cerrarse exteriormente y así prolongar el actual estado de cosas, trae consigo la inevitable consecuencia del retraso en la carrera tecnológica y por lo tanto la incompetencia de nuestras estructuras jurisdiccionales frente a estos temas.

(30) Para un mayor desarrollo de la actitud de los operadores jurídicos frente a las tecnologías disruptivas, ver Acciari, Hugo A. en "Smart Contracts, criptomonedas y el Derecho", LL 2/5/2019, 1; cita online: AR/DOC/1017/2019.

Aquí encontramos entonces el desafío de todos nosotros como operadores del mundo jurídico. Estas limitaciones seguramente irán disminuyendo con el desarrollo de la técnica en general, y con la inteligencia artificial en particular, pero desde ya obligan a los operadores jurídicos a trabajar en conjunto con profesionales de disciplinas no jurídicas —procesadores de datos, programadores, etc.— y a realizar esfuerzos que antes no eran necesarios.

Es por ello por lo que los abogados estamos obligados a salir de la concepción clásica y decimonónica del Derecho en la que hemos sido instruidos en nuestras universidades.

La búsqueda de mayor seguridad jurídica, menor cantidad de trámites (desburocratización) y la resolución de la mayoría de las situaciones de duda por medio de medios informáticos automáticos, busca también bajar la conflictividad y la litigiosidad. Es un desafío para evitar controversias y contribuir a la paz social a través de mecanismos que garanticen previsibilidad.

Sin dudas, al programar un gran número de respuestas se reducirán considerablemente las posibilidades de conflicto extrajudicial y judicial, pero ello no quita que a la vez esta figura pueda considerarse como un "phármakon", es decir, como un remedio y veneno al mismo tiempo. Si bien nos traerá la celeridad y certeza en las soluciones por contar con decisiones anticipadas, por otro lado, ante la rigidez, inflexibilidad e inalterabilidad que traen consigo, hay ciertas vicisitudes o incidencias que de configurarse volverían un tanto injusta la autoejecución del contrato en la forma pactada, evidenciando de esta manera la insuficiencia o —mejor dicho— la necesidad del complemento humano para una razonable valoración del caso.

La Privacidad Digital

DIEGO FERNÁNDEZ (*)

I. Introducción

En las últimas décadas, los avances tecnológicos no solo han cambiado la forma en la que los individuos se relacionan entre sí, sino que han permitido nuevas formas en las que la privacidad puede verse afectada. La barrera que distinguía al mundo físico de lo que hoy se nos presenta como uno digital se va perdiendo o desapareciendo, lo que nos obliga a repensar las protecciones tradicionales a la privacidad con una mirada sobre este nuevo escenario digital.

En esencia, el problema que plantea la tecnología es que las regulaciones o construcciones con las que nos hemos manejado durante mucho tiempo en algunos escenarios ya no responden a esta nueva realidad tecnológica. Esto hace que sean necesarias nuevas reglas o bien nuevas interpretaciones que se ajusten mejor a las nuevas realidades y, como sabemos, los cambios legales suelen ser más lentos que el avance tecnológico.

En este sentido, por ejemplo, la Corte Interamericana de Derechos Humanos tiene dicho que la fluidez informativa que existe en la actualidad coloca al derecho a la vida privada de las personas en una situación de mayor riesgo debido a las nuevas herramientas tecnológicas y su utilización cada vez más frecuente. En consecuencia, la CIDH consideró que resulta necesario que el estado asuma un mayor compromiso a fin de adecuar a los tiempos actuales las fórmulas tradicionales de protección del derecho a la vida privada (1).

Las nuevas tecnologías han puesto de nuevo el foco en preguntarnos qué significa la privacidad y la intimidad, cómo deben ser protegidas y, en consecuencia, cuándo es esperable tener una expectativa razonable de privacidad.

La injerencia sobre la privacidad en el contexto de la tecnología actual se da a través de los puntos de acceso a la información, como por ejemplo computadoras, dispositivos móviles, televisores inteligentes y múltiples dispositivos conectados al Internet de las Cosas.

Hoy ya no resulta una sorpresa el hecho de que al conectarnos a Internet vamos dejando un rastro de nuestras actividades que puede ser utilizado de distintas maneras, con o sin nuestro consentimiento. La preocupación que todo esto genera es que, a través de los dispositivos digitales y la información que por ellos transita,

(*) Abogado (UCA). Master en Leyes por la John Marshall Law School, Chicago. Profesor Universidad Di Tella del Programa de Educación Ejecutiva sobre Protección de Datos Personales. Profesor invitado sobre Privacidad Global de la John Marshall Law School. Socio del Departamento de Propiedad Intelectual, Nuevas Tecnologías y Privacidad de Marval, O'Farrell & Mairal.

(1) Corte Interamericana de Derechos Humanos, "*Escher y otro c. Brasil*", Serie C N° 220, 6 de junio de 2009.

se puede vigilar la vida privada e intimidad de las personas.

En este escenario, se analiza cómo debiera aplicarse la protección a la privacidad de los individuos frente al avance de nuevas tecnologías. Muchos entienden que la privacidad como la conocemos se encuentra en riesgo ya que toda esta información que se obtiene de los dispositivos digitales puede afectar negativamente la vida de los individuos de múltiples maneras.

Así, por ejemplo, muchos analistas sostienen que el uso de datos personales con fines electorales que hizo *Cambridge Analityca,* una consultora política que por varios años utilizó datos obtenidos de perfiles de redes sociales de millones de personas con fines de propaganda política para persuadir y/o modificar las opiniones de estas personas, afectó la democracia de los Estados Unidos.

Relacionado con la importancia de los datos en general, John Ellis argumenta en su libro *"The Zero Dollar Car"* que en un futuro cercano podremos, por ejemplo, pagar el alquiler de un automóvil mediante el consentimiento para que recojan nuestros datos al usarlo y los utilicen. Esto no debiera ser una práctica extraña ya que, al utilizar muchos de los servicios denominados ´gratuitos´, como por ejemplo buscadores o redes sociales, estamos autorizando el uso de nuestros datos a cambio de poder utilizar el servicio. John Ellis propone hacer este intercambio de forma más visible y consensuada.

Aún más, una investigación reciente de la publicación Vice descubrió que algunas empresas de telecomunicaciones de los Estados Unidos venden los datos de geolocalización de sus clientes a distintos terceros (agregadores de información), quienes luego los revenden a cualesquiera otros terceros. En igual sentido, el New York Times realizó una investigación en la que concluye que 17 de las 20 *apps* investigadas enviaban información de geolocalización a 70 compañías(2). Otra investigación del año 2013(3) analizó la información de geolocalización de 1.5 millones de personas durante un lapso de 15 meses y con cuatro datos de ubicación pudo identificar correctamente a la persona correspondiente sin saber su identidad de antemano.

Lo anterior muestra la importancia de los datos y las posibles implicancias que su utilización puede tener respecto de la privacidad de las personas.

Tradicionalmente, se ha sostenido que las medidas que importan una intromisión en la vida privada de las personas, como por ejemplo los allanamientos de sus hogares o la interceptación de su correspondencia o comunicaciones, requieren de la intervención y orden de un juez competente. Esto se traduce en la expectativa razonable de privacidad que el individuo tiene en espacios privados como sus hogares, su correspondencia y sus comunicaciones. De acuerdo con lo que venimos analizando, el derecho a la privacidad se debe extender y adaptar al nuevo contexto digital, en particular reconociendo el rol fundamental que la tecnología tiene en la vida actual de las personas, lo que implica que estas no puedan optar por no usarlas.

Antes de analizar las discusiones jurídicas acerca del derecho a la a privacidad en su interrelación con las nuevas tecnologías, analizaremos brevemente el contexto de tecnología en el cual se dan estas discusiones.

De acuerdo con un informe publicado recientemente por We Are Social y Hootsuite, con información proporcionada por GlobalWebIndex, GSMA Intelligente, Statista, Locowise, App Annie y SimiliarWeb, de los más de 7 billones de habitantes del mundo, 5 billones son usuarios únicos de dispositivos móviles –con una penetración del 67%– y existen un poco más de 4 billones de usuarios de Internet –con una penetración del 57%–, y con un crecimiento de 2,0% y 9,1% respectivamente en relación con enero

(2) Valentino-DeVries, J. - Singer, N. - Keller, M. H. - Krolik, A., "Your Apps Know Where You Were Last Night, and They´re Not Keeping It Secret", *The New York Times* (edición digital), 10 de diciembre de 2018.

(3) De Montjoye Y. - Hidalgo, C. A. - Verleysen, M. - Blondel, V. D., "Unique in the Crowd: The privacy bounds of human mobility", *Springer Nature* (edición digital), (25 de marzo de 2013).

del 2018 (4). El mismo informe detalla que, solo en Argentina, para los 44 millones de habitantes existen 60 millones de líneas de telefonía celular y 41 millones son usuarios de Internet (5).

Lo que este informe muestra, como también lo hacen muchos otros, es que en la práctica una gran parte de la población mundial tiene en su bolsillo o cartera un dispositivo que permite no solo ubicarlos en tiempo real y saber muchísimo acerca de sus conductas y preferencias, sino también reconstruir históricamente esta información en distintos momentos. Además, existe una clara tendencia al aumento en la cantidad y la precisión de la información recolectada, lo que hace que todos estemos virtualmente ubicados en tiempo y espacio durante la mayor parte del día.

Por otro lado, los datos que se pueden recolectar a través de dispositivos móviles resultan extremadamente valiosos en el marco de investigaciones judiciales, sobre todo en el marco de investigaciones y juicios penales. Pueden ayudar a establecer que un determinado sospechoso se encontraba en el lugar donde se cometió un delito mientras este sucedía. Por lo tanto, resulta razonable que las autoridades tengan un interés válido en querer acceder a estos datos.

En tales casos, la cuestión radica entonces en determinar cómo debe balancearse el derecho a la privacidad de los individuos frente al acceso de las autoridades a sus datos y qué resulta razonable exigir para que este acceso sea legítimo.

La privacidad es el derecho que todas las personas tienen a ser dejadas solas, sin intromisión de terceros, incluyendo al Estado, sin su voluntad y consentimiento. Por supuesto, este derecho no es absoluto y existen supuestos en los que otros derechos priman por sobre el derecho individual a la privacidad.

En nuestro país, la privacidad está regulada principalmente por el art. 19 de la Constitución Nacional, por el art. 1770 del Cód. Civ. y Com. (6), y por los arts. 150 (violación de domicilio) y 153 (violación de secretos y de la privacidad) del Cód. Penal, en conjunto con una gran cantidad de sentencias judiciales que han analizado casos y circunstancias específicas. Los dos primeros artículos establecen lo siguiente:

> Las acciones privadas de los hombres que de ningún modo ofendan al orden y a la moral pública, ni perjudiquen a un tercero, están sólo reservadas a Dios, y exentas de la autoridad de los magistrados. Ningún habitante de la Nación será obligado a hacer lo que no manda la ley, ni privado de lo que ella no prohíbe" (artículo 19 de la Constitución Nacional)"; y "El que arbitrariamente se entromete en la vida ajena y publica retratos, difunde correspondencia, mortifica a otros en sus costumbres o sentimientos, o perturba de cualquier modo su intimidad, debe ser obligado a cesar en tales actividades, si antes no cesaron, y a pagar una indemnización que debe fijar el juez, de acuerdo con las circunstancias *(…)* (art. 1770 del Cód. Civ. y Com.).

Dentro de este marco, por mucho tiempo los tribunales han resuelto distintos litigios relacionados con la privacidad de las personas.

A modo de ejemplo, podemos citar el reconocido fallo "Halabi" (7) de la Corte Suprema de Justicia de la Nación. En este caso, más todo su aporte respecto de los derechos de incidencia colectiva, el Máximo Tribunal sostuvo que "Acerca de estas situaciones este Tribunal ha subrayado que sólo la ley puede justificar la intromisión en la vida privada de una persona, siempre que medie un interés superior en res-

(4) Kemp, S., "Digital 2019: Global Internet Use Accelerates", *We Are Social,* 30 de enero de 2019.

(5) N/A. "Digital 2019: Argentina", recuperado de: *https://datareportal.com/reports/digital-2019-argentina* (último acceso 30 de julio de 2019).

(6) Que reemplazó el art. 1071 bis del Cód. Civ. que, de forma muy similar, establecía "El que arbitrariamente se entrometiere en la vida ajena, publicando retratos, difundiendo correspondencia, mortificando a otros en sus costumbres o sentimientos, o perturbando de cualquier modo su intimidad, y el hecho no fuere un delito penal, será obligado a cesar en tales actividades, si antes no hubieren cesado, y a pagar una indemnización que fijará equitativamente el juez, de acuerdo con las circunstancias; además, podrá éste, a pedido del agraviado, ordenar la publicación de la sentencia en un diario o periódico del lugar, si esta medida fuese procedente para una adecuada reparación".

(7) Fallos: 332:111.

guardo de la libertad de los otros, la defensa de la sociedad, las buenas costumbres o la persecución del crimen (Fallos: 306:1892; 316:703, entre otros). Es en este marco constitucional que debe comprenderse, en el orden del proceso penal federal, la utilización del registro de comunicaciones telefónicas a los fines de la investigación penal que requiere ser emitida por un juez competente mediante auto fundado (confr. art. 236, segunda parte, del Código Procesal Penal de la Nación, según el texto establecido por la ley 25.760), de manera que el común de los habitantes está sometido a restricciones en esta esfera semejantes a las que existen respecto a la intervención sobre el contenido de las comunicaciones escritas o telefónicas. Esta norma concuerda con el artículo 18 de la ley 19.798 que establece que ´la correspondencia de telecomunicaciones es inviolable. Su interceptación sólo procederá a requerimiento de juez competente ´".

Es decir, la Corte Suprema establece lineamientos claros respecto de cuándo se justifica la intromisión en la vida privada de las personas, indicando que debe mediar un interés superior en resguardo de la libertad de otros, la defensa de la sociedad, las buenas costumbres y –por supuesto- la persecución del crimen.

Asimismo, en un fallo del fuero penal en una causa en la que se investigaba la posible comisión de un delito por un empleado y, en ese marco, el tribunal consideraba la privacidad de las comunicaciones electrónicas del investigado, la Sala I de la Cámara Criminal y Correccional recordó en primer lugar lo sostenido en Fallos: 318: 1894 cuando se afirmó que "para restringir válidamente la inviolabilidad de la correspondencia, supuesto que cabe evidentemente extender al presente, se requiere: a) que haya sido dictada una ley que determine los "casos" y los "justificativos" en que podrá procederse a tomar conocimiento del contenido de dicha correspondencia; b) que la ley esté fundada en la existencia de un sustancial o importante objetivo del Estado, desvinculado de la supresión de la inviolabilidad de la correspondencia epistolar y de la libertad de expresión; c) que la aludida restricción resulte un medio compatible con el fin legítimo propuesto y d) que dicho medio no sea más extenso que lo indispensable para el aludido logro. A su vez, fines y medios deberán sopesarse con arreglo a la interferencia que pudiesen producir en otros intereses concurrentes (8)".

Asimismo, el tribunal continuó afirmando que "(…) una sociedad vigilada se transforma en una sociedad conformista y pasiva que aliena al mismo sistema democrático. De ahí que la protección constitucional de zonas de privacidad de la información personal que aseguran nuestra autonomía individual sea garantía del carácter democrático y, por tanto, valor constitutivo de las actuales sociedades tecnológicas".

Como vemos, y sin intención de agotar este tema que cuenta con muchísimos precedentes muy interesantes, existen límites claros a los fines de proteger la privacidad de las personas. Pero la mayoría de estos precedentes se han limitado a analizar casos en los que la privacidad es afectada por acciones en el mundo físico, como los allanamientos de domicilio y la toma de fotografías en lugares privados. Muy pocos han debido analizar el fenómeno de la privacidad digital.

Y dentro de la privacidad digital, como hemos visto, existe un interés muy marcado respecto de la geolocalización de las personas, muy en particular respecto de la geolocalización a través de la conexión de los dispositivos móviles a las antenas celulares de los distintos prestadores de servicios de telecomunicación.

Sobre esto último, la geolocalización a través de celdas celulares, existen un debate muy interesante en los Estados Unidos y, como consecuencia de este debate y un fallo de la Corte Suprema de los Estados Unidos, ha comenzado también un debate en nuestro país.

II. La geolocalización en los Estados Unidos

En los Estados Unidos, la tensión entre las investigaciones policiales y el derecho a la privacidad de los ciudadanos se traduce en una discusión acerca de la necesidad o no de contar con un *warrant*, una orden judicial que llegue al estándar de "causa probable" (*probable cause* en inglés). Este estándar es el que se requiere

(8) Cámara Nacional Criminal y Correccional, Sala I, "Gotlib Saúl y otros", 13 de febrero de 2015.

para la emisión de una orden de intervención telefónica o una orden de allanamiento, por ejemplo.

La Cuarta Enmienda de la Constitución de los Estados Unidos protege a los individuos de los registros irrazonables (*unreasonable searches* en inglés (9)), y resguarda su derecho a la privacidad. De acuerdo con la jurisprudencia norteamericana, cuando existe una expectativa de privacidad que la sociedad considera razonable, cualquier registro que realicen las autoridades requiere que un juez emita una orden judicial basada en una causa probable de la comisión de un delito.

Sin embargo, esto genera interrogantes acerca de a qué tipo de registros se refiere la Cuarta Enmienda y cuándo existe una expectativa razonable de privacidad. Es evidente que, originalmente, el texto fue ideado para proteger a las personas en el caso de registros físicos, como el allanamiento de sus hogares o el acceso a sus papeles privados. Sin embargo, en el contexto actual y teniendo en cuenta el avance de la tecnología, los tribunales debieron comenzar a analizar si esta protección pensada para un mundo físico debía extenderse del mismo modo al mundo digital, muy en particular en lo que hace a la información y datos generados por los dispositivos móviles.

En 2014, en el caso "*Riley v. California*" (10) la Corte Suprema de los Estados Unidos extendió la protección que garantiza la Cuarta Enmienda de su Constitución a la información digital contenida en teléfonos celulares de personas que habían sido arrestadas. La Corte Suprema de los Estados Unidos estableció que los teléfonos celulares son una parte tan importante y constitutiva de la vida diaria que contar con uno resulta esencial para la participación de las personas en la sociedad moderna.

Más tarde, ya en 2018, la Corte Suprema de los Estados Unidos se expidió por primera vez de forma expresa acerca del uso de los datos de geolocalización en relación con el derecho constitucional a la privacidad en *Carpenter* (11). Se argumentó que resultaba inadmisible como prueba la información de geolocalización obtenida del teléfono celular del acusado alegando que tal acceso había constituido una violación a su derecho constitucional a la privacidad.

El voto de la mayoría, compuesta por cinco de los nueve jueces, estableció que la información de geolocalización obtenida de las conexiones que un teléfono celular hace a las distintas celdas de conexión implica un registro a efectos de la Cuarta Enmienda y que los usuarios de teléfonos celulares cuentan con una razonable expectativa de privacidad.

En particular, destacó que la información de geolocalización de dispositivos móviles implica un mayor peligro para la privacidad en aquellos dispositivos que incluyen un GPS debido a que hoy en día todos llevamos teléfonos celulares con nosotros a toda hora, por lo que los datos sobre la ubicación de estos dispositivos son la forma perfecta de vigilancia. Además, estos datos no solo muestran una ubicación actual, sino que permiten reconstruir la ubicación en tiempo y espacio hacia el pasado, permitiendo en general determinar la ubicación varios meses o incluso años atrás.

En síntesis, la Corte Suprema de los Estados Unidos estableció que, en el caso de información de geolocalización de dispositivos móviles, se debe aplicar el mismo estándar que se requiere en caso de allanamientos (12).

III. Efectos de *Carpenter* en la Argentina

Lo discutido en *Carpenter* tuvo repercusión mundial, alentando el debate sobre la privacidad digital. Como muestra de ello, en septiembre de 2018, un Juzgado Penal, Contravencional y de Faltas de la Ciudad de Buenos Aires dictó dos resoluciones que citan a *Carpenter* y refle-

(9) Este término no tiene una traducción exacta al español y hemos optado por utilizar "registro irrazonable" a efectos de este artículo.

(10) Corte Suprema de Estados Unidos, "*Riley c. California*", 573 U.S. (2014).

(11) Corte Suprema de Estados Unidos, "*Carpenter c. United States*", 585 U.S. (2018).

(12) Para más información sobre este caso, ver Fernández, Diego y O'Farrell, Inés, "Privacidad en el contexto digital: la geolocalización de dispositivos móviles", Suplemento #LegalTech de Thomson Reuters - La Ley, p. 87.

jan su razonamiento.(13) En ambos casos, el tribunal declaró la nulidad de las medidas dispuestas por los fiscales en el contexto de dos investigaciones penales, que consistían en pedidos de informes cursados a empresas de telecomunicaciones en relación con distintas líneas telefónicas e incluían una solicitud de adjuntar un listado de aquellas celdas de conexión que hubieran sido habilitadas por el dispositivo, con su correspondiente ubicación geográfica. En pocas palabras, el tribunal concluyó que una medida de este tipo, que implicaba conocer con cierta exactitud la ubicación de un dispositivo móvil a través de las celdas de conexión –y que por consiguiente permitía en principio conocer la ubicación del titular del dispositivo– no podía ser ordenada por un fiscal, sino que se requería una orden judicial.

Sostuvo que los fiscales se encuentran habilitados para requerir autónomamente ciertos informes de acuerdo con el art. 93 del Código Procesal Penal de la Ciudad Autónoma de Buenos Aires, que dispone que a fin de desarrollar la investigación preparatoria los fiscales podrán citar a testigos, requerir los informes y peritajes que estimes pertinentes y útiles, practicar las inspecciones de lugares y cosas, disponer o requerir secuestro de elementos y todas las medidas que consideren necesarias para el ejercicio de sus funciones. Sin embargo, también destacó que el mismo artículo establece que se deberá solicitar orden judicial para practicar allanamientos, requisas o interceptaciones de comunicaciones o correspondencia.

En este sentido, el juzgado consideró que la información correspondiente a las celdas celulares de conexión de un determinado dispositivo móvil que permite establecer su ubicación geográfica se encuentra en una categoría de sensibilidad desde la perspectiva de la privacidad y que los usuarios tienen una razonable expectativa de privacidad respecto de ella.

En este caso, esto implicaría –según el tribunal— redimensionar el alcance del derecho a la intimidad y el alcance de la labor jurisdiccional. Eso se debe a que las medidas de prueba contempladas en las normas fueron ideadas exclusivamente para la investigación de hechos acontecidos en el mundo físico y no en el mundo digital.

En este contexto, el juzgado hizo hincapié en la necesidad de contar con una interpretación amplia y dinámica del derecho a la intimidad. Además, enfatizó sobre la importancia de una interpretación progresiva de la definición de "información personal almacenada" a efectos del art. 13.8 de la Constitución de la Ciudad Autónoma de Buenos Aires, que establece que el allanamiento de domicilio, las escuchas telefónicas, el secuestro de papeles y correspondencia o información personal almacenada solo pueden ser ordenados por el juez competente.

Por lo tanto, y luego de referirse a los hechos y argumentos del caso Carpenter, el juzgado consideró que correspondía declarar la nulidad del pedido de informe a las empresas de telefonía en lo referido a la solicitud del listado de celdas de conexión habilitadas y su correspondiente ubicación, ya que esto requeriría una orden judicial.

IV. ¿Cuál será el próximo paso?

Existe una gran cantidad de películas y novelas que tienen personajes principales cuyo superpoder es el de saber lo que el otro está pensando sin necesidad de interacción.

Si bien esto fue siempre parte de historias de ciencia ficción, pareciera que se está avanzando, aún en un estado embrionario, hacia una realidad en la que esto pudiera volverse posible.

En ese sentido, el reconocido neurólogo Facundo Manes –refiriéndose a la posibilidad de que los avances de la ciencia y la tecnología permitan leer los pensamientos de los demás— sostiene que "(…) es analizando estos patrones de actividad que las neurociencias han comenzado a avanzar en hipótesis sobre qué es lo que estamos pensando, viendo, imaginando o escuchando. Esta información es procesada por una computadora que a través de un programa, llamado ´clasificador´, aprende a asociar pa-

(13) Juzgado Penal, Contravencional y de Falta N° 10 de la Ciudad de Buenos Aires, Expediente N° 24452/18, registro interno 1429, 3 de septiembre de 2018; y Expediente N° 25380/18, registro interno 1435, 4 de septiembre de 2018.

trones de actividad cerebral con distintos estímulos. Una vez que el programa adquirió suficientes datos para aprender a diferenciar estos patrones, podría deducir lo que piensa o ve alguien" (14).

En igual sentido, en un estudio de 2017 publicado por Marcello Ienca y Roberto Andorno (15), refiriéndose a la idea de que la mente y los pensamientos son el último refugio de la libertad personal y de la autodeterminación, se sostiene que, mientras que el cuerpo puede fácilmente ser objeto de dominación y control por otros, nuestra mente –junto con nuestros pensamientos, creencias y convicciones—, se encuentra más allá de restricciones externas. Sin embargo, se agrega, con los avances en ingeniería neural, mapeo cerebral y neuro-tecnología penetrante, puede ser que la mente no sea más esa fortaleza tal como la conocemos.

Todo esto indica que, así como la privacidad digital generó reformular y volver a analizar las soluciones desarrolladas para la privacidad en el mundo físico, es probable –si las neurociencias y tecnologías siguen avanzando como muchos creen—, que debamos volver a reformular todos estos conceptos nuevamente porque la privacidad tal como la conocemos –aún la digital— podría cambiar sustancialmente.

Estos últimos autores agregan que, en su opinión, este nuevo escenario podría hacer nacer nuevos derechos fundamentales, tales como el derecho a la libertad cognitiva, el derecho a la privacidad mental, el derecho a la integridad mental y el derecho de continuidad psicológica.

V. Conclusión

Como hemos visto, la posible afectación a la privacidad de las personas relacionada con las nuevas tecnologías es algo que se encuentra en plena discusión y constante evolución y está lejos de estar zanjada.

Frente a los avances tecnológicos, la respuesta jurisprudencial ha sido la de intentar preservar el mismo grado de protección de la privacidad que el existente al momento de la adopción del texto constitucional, pero adaptado a los tiempos actuales.

Esta discusión está aún en una etapa inicial y será necesario seguir analizando los avances tecnológicos y las soluciones legales tradicionales.

(14) Manes, Facundo y Niro, Mateo, *El cerebro del futuro. ¿Cambiará la vida moderna nuestra esencia?*, Planeta, ps. 93 y ss.

(15) Ienca, Marcello y Andorno, Roberto, "Towards new human rights in the age of neuroscience and neurotechnology", *Life Sciences, Society and Policy,* 2017.

Los desafíos jurídicos del *big data*. Tensiones de derechos entre la parametrización analítica, la toma automatizada de decisiones, el *targetting* y el perfilamiento

JOHANNA CATERINA FALIERO (*)

I. Introducción

No es necesario ahondar *brevitatis causae* en la revolución que la introducción de las TICs ha causado irreversiblemente en nuestras vidas, ni cómo cada vez se procesan mayores volúmenes de información con una mayor velocidad de procesamiento y cómo los flujos de información intensificados dan lugar a más vías y canales de comunicación y modos de relacionamiento. Esos simplemente son hechos de la realidad que nos circunda.

Todo ello es sabido, es innegable y resulta claramente inobjetable. Lo que aún no discutimos de un modo conciso y con la profundidad conceptual que merece es la introducción masiva de complejas técnicas riesgosas de procesamiento de datos, cuyos peligros se desconocen y exceden a sus propios creadores y artífices, fenómeno que clarísimamente también nos excede desde lo jurídico y del cual debiéramos ocuparnos urgentemente por la responsabilidad que tenemos como operadores respecto de la evitación de sus consecuencias dañosas, irreversibles e incontenibles.

Técnicas tales como *big data, data mining*, inteligencia artificial, *machine learning* y *deep learning*, aunque no logren aún ser todo lo inteligentes y autónomas que imaginamos propiamente para el futuro distópico que sí alcanza a asustarnos, sí son lo suficiente y tangiblemente riesgosas y peligrosas para aquello que concebimos por privacidad y seguridad de datos, lo que podría convertir a estos dos derechos y principios en utopías irrealizables desde lo técnico y daría consecuentemente por resultado la necesidad jurídica de su negación por imposibilidad fáctica de su realización.

Es así como tantos operadores jurídicos hoy día sucumben progresivamente a la protección que principiológicamente alguna vez los inspiró a pronunciarse avasallados por la realidad y bregando por ceder en sus estándares

(*) Consultora Internacional, Asesora y Representante Legal Especializada para Argentina, LATAM, Caribe y UE en Derecho Informático, *Data Privacy, Data Protection, Data Governance* y *Compliance*, *Infosecurity*, Ciberseguridad, Criptomonedas, *Blockchain Technology,* Contratación Electrónica, *E-commerce*, Economía Digital, *Smart Contracts*, entre otras temáticas. Directora de Faliero Attorneys At Law. Es Doctoranda y Especialista en Derecho Informático y Abogada en Derecho Empresarial y Privado (F. Derecho, UBA). Directora de Posgrados y Profesora Titular de Grado y Posgrado (F. Derecho, UBA; F. Ingeniería, UNDEF; F. Derecho, USAL; F. Derecho y F. Ingeniería, UP; F. Derecho y F. Ingeniería, UCA; ADACSI-ISACA Bs.As. Chapter), Investigadora Adscripta Inst. Gioja, UBACyT, DeCyT y PII, expositora nacional e internacional. Autora de: *Criptomonedas: la nueva frontera regulatoria del Derecho Informático* (Ad Hoc, 2017); *Historia Clínica Electrónica: El futuro de la gestión documental sanitaria en la era de la E-Salud* (Ad Hoc, 2018) y *El derecho al anonimato: revolucionando el paradigma de protección en tiempos de la postprivacidad* (Ad Hoc, 2019).

de privacidad por el solo anhelo de resolver las dicotomías jurídicas que los aquejan y la puja de intereses que subyacen a estos derechos y principios, lo que no es menos importante.

En la era de perfilamento, el titular del dato tiene una identidad digital mellada, una identidad digital disociada y determinística, que puede llegar a ser letal tanto para él mismo como para aquellos que lo sucedan. Al respecto de las consecuencias de las técnicas riesgosas de tratamiento, abundan las proyecciones cortoplacistas, pero poco se ha escrito respecto del impacto a mediano o largo plazo y no solo respecto del titular del dato, sino respecto de todos aquellos impactados directa o indirectamente por los datos del titular por relacionamiento e inferencia.

En líneas resumidas, este trabajo persigue abordar los desafíos jurídicos del *big data*: las tensiones de derechos entre la parametrización analítica, la toma automatizada de decisiones, el targetting y el perfilamiento, en la búsqueda de respuestas que sirvan para revitalizar la privacidad como derecho y revolucionarla en el reconocimiento de algo superador tanto desde lo jurídico como desde lo técnico.

II. La Protección de Datos Personales

La protección de los datos personales desde un punto de vista regulatorio ha sido una preocupación para el derecho de todas partes del mundo y desde tiempos inmemoriales. La moderna protección de los datos personales se inspira en un concepto de derecho superador al de privacidad e intimidad, que es el derecho a la autodeterminación informativa.

El derecho a la autodeterminación informativa es el derecho que posee todo individuo a proteger los datos personales que a él refieren y determinar, libremente y de manera autónoma, su reserva o destino y qué acciones pueda realizarse con y sobre ellos, lo cual adquirió creciente relevancia con la masificación del tratamiento informatizado de datos.

Con las técnicas de tratamiento citadas introductoriamente, muchas y en más de las veces se prescinde del respeto por la autodeterminación informativa de los titulares de los datos. A la hora de utilizar *big data, data mining*, inteligencia artificial, *machine learning* y *deep learning*, muy pocas o nulas veces se informa al titular del dato de su utilización, sino que solamente se informan las finalidades de tratamiento y no las técnicas que se utilizan para llegar a ellas, lo cual es sumamente parcial y abusivamente engañoso.

La autodeterminación informativa del titular solamente se puede ejercer correcta y válidamente cuando existe una información plena que inspira el consentimiento brindado por el titular para el tratamiento de sus datos. La información al respecto de estas técnicas riesgosas de tratamiento es opaca y superficial y, dada la complejidad que poseen las mismas, muchas veces se evade el deber *so pretexto* de la misma por desinformar por el exceso informativo que implicaría hacerlo adecuadamente, lo cual es paradójico.

En términos más simples, quienes utilizan estas técnicas de tratamiento tienen un claro conocimiento que, por sentido común y aversión al riesgo y peligro, el titular del dato en caso de ser informado adecuadamente retiraría su consentimiento o no lo brindaría, por lo que la opacidad informativa sirve para que acepte pasivamente aquello que, de ser conocido, nunca se aceptaría.

Dicho esto, no podemos permanecer impertérritos frente a este reconocimiento de una práctica abusiva generalizada e instalada en la industria de procesamiento, ni deberíamos ser cómplices de la estructuración y justificación legal de su perpetración. Muy por el contrario, deberíamos actuar y reconocer el riesgo intrínseco del procesamiento de datos bajo estas técnicas modernas y reconocer que existe un deber de precaución y de prevención del daño respecto de estas técnicas, un deber agravado de información al respecto de sus riesgos y una responsabilidad objetiva por los riesgos del desarrollo que tienen y se seguirán viendo y por aquellos que estén por descubrirse.

III. Parametrización Analítica, la Toma Automatizada de Decisiones el Targetting y el Perfilamiento

La era de la postprivacidad nos enfrenta a la parametrización analítica, la toma automati-

zada de decisiones, la utilización masiva del targetting para diversos fines (no solo publicitarios) y el perfilamiento a escala masiva, privado y público, de los titulares de los datos.

Las técnicas de tratamiento de datos que se utilizan en nuestros días son cada vez más complejas, profundas, minuciosas, incisivas, intrusivas e invasivas del individuo y del despliegue de su personalidad, elecciones, pareceres, actividades, características, etc.

De manera no taxativa y simplemente ejemplificativa, enunciaba el art. 40 del Anteproyecto de reforma de nuestra Ley de Protección de Datos Personales en su segunda versión como técnicas de tratamiento de datos que se entendían por altamente riesgosas —en términos de afectación de derechos fundamentales de los titulares por su naturaleza/alcance/contexto/finalidades, que hacían nacer de forma obligatoria la necesidad de efectuar la evaluación de impacto relativa a la protección de datos personales—,a las siguientes:

> … a) Evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento de datos automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar;
>
> b) Tratamiento de datos sensibles a gran escala, o de datos relativos a antecedentes penales o contravencionales;
>
> c) Tratamiento de datos mediante tecnologías que se consideren potencialmente invasivas de la privacidad, como la observación sistemática a gran escala de una zona de acceso público (videovigilancia), la utilización de aeronaves no tripuladas (drones), la vigilancia electrónica, la minería de datos, la geolocalización, el tratamiento de datos a gran escala, la denominada “Internet de las Cosas”; entre otras;
>
> d) Tratamiento significativo no incidental de datos de niñas, niños y adolescentes, o dirigido especialmente a tratar datos de los mismos.

En este sentido, la regulación europea en la que se inspiraba este listado correspondía a la recepción normativa en la Directiva 680/2016 y Reglamento 679/2016 de la evaluación de impacto relativa a la protección de datos.

El nuevo Reglamento europeo, en el art. 35 en su parte pertinente señala:

> ARTÍCULO 35: Evaluación de impacto relativa a la protección de datos
>
> 1.Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares.
>
> 2.El responsable del tratamiento recabará el asesoramiento del delegado de protección de datos, si ha sido nombrado, al realizar la evaluación de impacto relativa a la protección de datos.
>
> 3.La evaluación de impacto relativa a la protección de los datos a que se refiere el apartado 1 se requerirá en particular en caso de:
>
> a) evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar;
>
> b) tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, apartado 1, o de los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10, o
>
> c) observación sistemática a gran escala de una zona de acceso público.

> 4.La autoridad de control establecerá y publicará una lista de los tipos de operaciones de tratamiento que requieran una evaluación de impacto relativa a la protección de datos de conformidad con el apartado 1. La autoridad de control comunicará esas listas al Comité a que se refiere el artículo 68.
>
> 5.La autoridad de control podrá asimismo establecer y publicar la lista de los tipos de tratamiento que no requieren evaluaciones de impacto relativas a la protección de datos. La autoridad de control comunicará esas listas al Comité.
>
> 6.Antes de adoptar las listas a que se refieren los apartados 4 y 5, la autoridad de control competente aplicará el mecanismo de coherencia contemplado en el artículo 63 si esas listas incluyen actividades de tratamiento que guarden relación con la oferta de bienes o servicios a interesados o con la observación del comportamiento de estos en varios Estados miembros, o actividades de tratamiento que puedan afectar sustancialmente a la libre circulación de datos personales en la Unión…

El perfilamiento que se efectúa a través del procesamiento de datos, siendo *per se* una práctica que naturalmente es concebible como riesgosa, puede hacer en sí misma uso de otras múltiples prácticas absolutamente riesgosas para el individuo titular del dato.

La evaluación sistemática, exhaustiva y automatizada de los aspectos personales de los individuos es algo centralmente riesgoso porque ello siempre produce efectos jurídicos, puesto que constituye una afectación a derechos de la personalidad de ese individuo al mismo tiempo que siempre existe, como consecuencia de ello, una afectación a esa individualidad.

El *big data* o tratamiento de datos a gran escala y *data mining* son dos caras del mismo proceso ya que uno se encarga de procesar grandes masas de datos mientras que el otro se ocupa de extraer datos útiles de dichos procesamientos.

Respecto de la utilización de las técnicas de *big data* y *data mining*, tanto la inteligencia artificial, el *machine learning* o aprendizaje automático y el *deep learning* o aprendizaje profundo hacen uso de ellas.

La ley 25.326 de Protección de los Datos Personales, aún vigente y cuya reforma se proyecta, establece respecto de la formación de perfiles publicitarios:

> ARTICULO 27. — (Archivos, registros o bancos de datos con fines de publicidad).
>
> 1. En la recopilación de domicilios, reparto de documentos, publicidad o venta directa y otras actividades análogas, se podrán tratar datos que sean aptos para establecer perfiles determinados con fines promocionales, comerciales o publicitarios; o permitan establecer hábitos de consumo, cuando éstos figuren en documentos accesibles al público o hayan sido facilitados por los propios titulares u obtenidos con su consentimiento.
>
> 2. En los supuestos contemplados en el presente artículo, el titular de los datos podrá ejercer el derecho de acceso sin cargo alguno.
>
> 3. El titular podrá en cualquier momento solicitar el retiro o bloqueo de su nombre de los bancos de datos a los que se refiere el presente artículo."
>
> La misma norma, respecto de las valoraciones personales automatizadas establece la limitación que las decisiones judiciales o actos administrativos no pueden tener como único fundamento su resultado, lo cual quiere decir que, las mismos pueden parcialmente sustentarse en valoraciones personales automatizadas, pero no exclusivamente.
>
> "ARTICULO 20. — (Impugnación de valoraciones personales).
>
> 1. Las decisiones judiciales o los actos administrativos que impliquen apreciación o valoración de conductas humanas, no podrán tener como único fundamento el resultado del tratamiento informatizado de datos personales que

suministren una definición del perfil o personalidad del interesado.

2. Los actos que resulten contrarios a la disposición precedente serán insanablemente nulos.

Por su parte, el Proyecto de Reforma de la Ley de Protección de Datos Personales recepta como modalidad de obtención del consentimiento la forma tácita, lo que en tratamiento de datos es absolutamente riesgoso y debiera ser inadmisible desde el punto de vista de la protección de derechos.

ARTÍCULO 12.- Consentimiento. El tratamiento de datos, en cualquiera de sus formas, requiere del consentimiento libre e informado de su titular para una o varias finalidades específicas.

El consentimiento puede ser obtenido de forma expresa o tácita.

La forma del consentimiento depende de las circunstancias, el tipo de dato personal y las expectativas razonables del titular de los datos.

El consentimiento expreso, de acuerdo a las circunstancias particulares del tratamiento de datos del que se trate, puede ser obtenido por escrito, verbalmente, por medios electrónicos, así como por cualquier forma similar que la tecnología permita brindar.

Para el tratamiento de datos sensibles se requiere el consentimiento expreso, salvo las excepciones establecidas por ley.

El consentimiento tácito es admitido cuando surja de manera manifiesta del contexto del tratamiento de datos y la conducta del titular de los datos sea suficiente para demostrar la existencia de su autorización. Es admisible únicamente cuando los datos requeridos sean necesarios para la finalidad que motiva la recolección y se haya puesto a disposición del titular de los datos la información prevista en el artículo 15,

sin que éste manifieste su oposición. El tratamiento de datos ulterior debe ser compatible con las finalidades manifiestas que surgen del contexto que originó la recolección. En ningún caso procede para el tratamiento de datos sensibles.

En todos los casos, el responsable del tratamiento tiene la carga de demostrar que el titular de los datos consintió el uso de sus datos personales.

El art. 14 del Proyecto establece una peligrosa excepción al consentimiento y a los fines de la parametrización analítica una gran herramienta de auxilio:

ARTÍCULO 14.- Excepciones al consentimiento previo. No es necesario el consentimiento para el tratamiento de datos cuando se trate de listados cuyos datos se limiten a nombre y apellido, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento, domicilio y correo electrónico, ni para el tratamiento de la información crediticia en los términos del Capítulo 6.

En lo que respecta a las valoraciones personales automatizadas, el Proyecto de Reforma representa graves peligros en cuanto a la imposibilidad de oponerse a ser objeto de una decisión basada únicamente en ellas.

ARTÍCULO 32.- Valoraciones personales automatizadas. El titular de los datos tiene derecho a oponerse a ser objeto de una decisión basada únicamente en el tratamiento automatizado de datos, incluida la elaboración de perfiles, que le produzca efectos jurídicos perniciosos o lo afecte significativamente de forma negativa.

El titular de los datos no podrá ejercer este derecho si la decisión:

a. Es necesaria para la celebración o la ejecución de un contrato entre el titular de los datos y el responsable del tratamiento;

b. Está autorizada por Ley;

c. Se basa en su consentimiento expreso.

> En los casos a que se refieren los incisos a) y c), el responsable del tratamiento debe adoptar las medidas adecuadas para salvaguardar los derechos del titular de los datos.

Por último, el Proyecto de Reforma expande lo relativo a los perfiles publicitarios, lo cual resulta claramente riesgoso dada la contracción protectoria que vislumbra todo el texto de la norma.

> ARTÍCULO 68.- Bases destinadas a la publicidad. Pueden tratarse sin consentimiento de su titular datos personales con fines de publicidad, venta directa y otras actividades análogas, cuando estén destinados a la formación de perfiles determinados o que permitan establecer hábitos de consumo que categoricen preferencias y comportamientos similares de las personas, siempre que los titulares de los datos sólo se identifiquen por su pertenencia a tales grupos genéricos, con más los datos individuales estrictamente necesarios para formular la oferta a los destinatarios.
>
> En toda comunicación con fines de publicidad que se realice por correo, teléfono, correo electrónico, Internet u otro medio que permita la tecnología en el futuro, el responsable o encargado del tratamiento debe implementar medidas razonables que informen al titular de los datos la posibilidad de ejercer los derechos previstos en la presente Ley.
>
> Los datos referentes a la salud sólo pueden ser tratados, a fin de realizar ofertas de bienes y servicios, cuando hubieran sido obtenidos de acuerdo con la presente Ley y siempre que no causen discriminación, en el contexto de una relación entre el consumidor o usuario y los proveedores de servicios o tratamientos médicos y entidades sin fines de lucro. Estos datos no pueden cederse a terceros sin el consentimiento previo, expreso e informado del titular de los datos. A dicho fin, éste debe recibir información clara y suficiente respecto del carácter sensible de los datos que proporciona y de que no está obligado a suministrarlos, junto con la información prevista en el artículo 15 y la mención de su derecho a oponerse al tratamiento de sus datos.
>
> En los supuestos contemplados en el presente artículo, el titular de los datos puede ejercer el derecho de acceso sin cargo ni limitación temporal alguna. La información a suministrársele debe incluir la fuente de la que se obtuvieron sus datos, indicando, en su caso, el nombre del responsable o encargado del tratamiento que proveyó la información.

Dado el marco regulatorio presente y futuro analizado, se colige que la toma de decisiones automatizadas y el perfilamiento como práctica se encuentran instalados, y dados los pocos condicionamientos protectorios, la parametrización analítica que se alcanza a través de las complejas y casi ni mencionadas técnicas de procesamiento y el *targetting* que se despliega a través de su implementación encuentran pocos reparos, límites y responsabilidades prefijadas en estos contextos legales.

IV. El derecho humano al anonimato

La privacidad requiere de una revolución dado que, en el contexto fáctico y regulatorio analizado, no es posible proteger lo concebido por la misma con las herramientas disponibles y ya exploradas en materia tuitiva.

De allí que, frente a la imposibilidad de contener las consecuencias del procesamiento automatizado de datos por las modernas y riesgosas técnicas de procesamiento, surge la necesidad de evitar técnica y legalmente la recopilación, almacenamiento, generación y procesamiento innecesario y potestativo de datos, cuyo control de otro modo es ingobernable.

El anonimato como respuesta es sinónimo de libertad y representa el desdoblamiento más revolucionario de la privacidad en entornos de control, perfilamiento, parametrización y vigilancia extrema, puntillista, sistemática y generalizada.

El derecho a la privacidad e intimidad del individuo como derechos humanos fundantes

que inspiraron la regulación protectoria en materia de datos personales y que dieron origen a la construcción del concepto y derecho de autodeterminación informativa del titular hoy día se encuentran en jaque. La privacidad se encuentra hace largo tiempo deteriorada y, aún sin nuestro reconocimiento expreso, ha dejado de existir como alguna vez se la conoció y resulta desde lo técnico cuasi inconcebible.

En tiempos de la postprivacidad, los individuos somos maquinarias de producción cuasi industrial de datos que definen y delinean nuestra identidad digital. La privacidad nace derrotada en los entornos actuales de procesamiento y las amenazas y conculcaciones a las que se encuentra expuesta tienen tanto origen ilícito como lícito. No solo proviene el interés de penetrar en nuestros datos por parte de las empresas, sino también de los mismos Estados.

El anonimato es el derecho por excelencia en una sociedad inmersa en un paradigma de postprivacidad en el que se utilizan técnicas modernas de tratamiento automatizado de datos bajo las múltiples técnicas existentes que de manera cada vez más eficiente transgreden los límites de lo que alguna vez concebimos por privado.

De allí la urgencia de erigir una teoría del derecho al anonimato como derecho humano al igual que el derecho a la protección de datos en tiempos de la postprivacidad, revolucionando el paradigma protectorio en la materia, lo que aún para muchos resulta no solo inconcebible sino hasta potencialmente ilícito.

El individuo titular del dato postprivado merece ser anónimo para preservar su dignidad, libertad, unicidad, individualidad, identidad y proyecto de vida, entre otros derechos humanos.

La parametrización, la sobreexposición del individuo, el conocimiento absoluto, su identidad digital y no digital, la trazabilidad de su persona, la capacidad de identificación, el perfilamiento al que es permanentemente sometido, el sometimiento de sus datos a técnicas de tratamiento cada vez más invasivas/agresivas/intrusivas/vejatorias/intimidatorias/discriminatorias/conculcatorias/peligrosas, y la incapacidad fáctica, jurídica y técnica que tiene el mismo individuo de gobernar la totalidad de datos y metadatos que puedan ser asociados e identificados con su persona, son los mayores peligros a los cuales nos encontramos sometidos y de los cuales no podemos escapar si no hay cambios en lo legal que admitan posibilidades protectorias impensadas hasta el momento.

El derecho humano al anonimato representa la única solución técnico-jurídica superadora que impediría la no regresividad del mismísimo derecho a la privacidad por la contracción fáctica a la cual se encuentra sometido.

El anonimato es indudablemente el derecho humano fundamental por excelencia que inspira, junto con la libertad y autonomía de la voluntad, la edificación de la revolución de la protección de datos en la era de la postprivacidad(1).

V. Conclusión y reflexiones

No resulta necesario ser un experto en *data science* para afirmar que las técnicas de *big data, data mining,* inteligencia artificial, *machine learning* y *deep learning*, entre otras técnicas riesgosas de procesamiento de datos, engendran peligros incontenibles que no necesitamos llegar a verificar en cada caso en concreto, sino simplemente proyectar por lógica del razonamiento, ya que por principio de prevención y precaución no requerimos que se materialice el daño ni debemos permitir que se incremente, sino evitarlo cuando hay certeza o sospecha que pueda llegar a existir.

Las técnicas citadas requieren, para su funcionamiento de datos, una cantidad inmensa de los mismos, un relacionamiento complejo de estos, la generación de datos relacionales y subproductos de procesamiento que desconocemos, que permiten reflejar digitalmente por medio de la parametrización automatizada y el perfilamiento, aspectos de nuestras preferencias, conductas, hábitos, personalidad y demás aristas personalísimas de nuestra individuali-

(1) Faliero, Johanna Caterina, *El derecho al anonimato: revolucionando el paradigma de protección en tiempos de la postprivacidad,* Ad Hoc, Argentina, 2019.

dad que nosotros podemos no querer divulgar o bien desconocemos sobre nosotros mismos y que nos exponen a peligros que no podemos conmensurar al momento del perfilamiento.

La parametrización no es solo tensión de derechos, nos vuelve vulnerables, nos expone a peligros de los que no podemos escapar una vez realizada. El volumen de datos y la complejidad del relacionamiento de los mismos, sumada a la incapacidad de contener la distribución física y lógica de los mismos y la imposibilidad de circunspección de sus daños, permite arriesgar que, por principio precautorio, al respecto de estas técnicas listadas como otras que surjan, debemos tomar medidas proactivamente que inhiban la expansión del peligro que representan.

Proyectivamente, quienes trabajan con estas técnicas desconocen la verdadera potencialidad y confines de su propia capacidad, por lo que, simplemente, la imposibilidad de encasillar su magnitud y capacidad de estudiar genuinamente su impacto debería servir como justificativo sobrado para minimizar su utilización y prohibir su explotación irrestricta con fines potestativos.

En los contextos actuales de procesamiento o tratamiento de datos, la privacidad es una ficción que se mantiene y preserva mientras que respeten las condiciones de su cumplimiento, lo que resulta absolutamente frágil y endeble. Por lo que, el derecho humano al anonimato en aquellos ámbitos en los que legalmente podamos serlo y en los que jurídicamente no se requiera nuestra capacidad de identificación por la protección de otros derechos y finalidades jurídicas legalmente protegidas, reconocidas y receptadas, es nuestra elección y señorío irrenunciable y debiera ser reconocido como un límite natural a la proliferación y expansividad de las modernas y riesgosas técnicas de procesamiento.

Los desafíos jurídicos del *big data* son múltiples y las tensiones de derechos que se generan entre la parametrización analítica, la toma automatizada de decisiones, el *targetting* y el perfilamiento son innegables y cada vez más expansivas y dañinas, por lo que es nuestro deber intensificar la protección de datos en los contextos de tratamiento postprivado y revolucionar los extremos protectorios de la privacidad para su preservación.

Las personas jurídicas en el nuevo derecho y tecnología. Bienvenidos los robots

JUAN ANTONIO TRAVIESO (*)

I. Introducción

El derecho del siglo pasado no presentaba grandes cambios.

La persona física y sus derechos fueron producto de desarrollos doctrinarios seculares. La sociedad se iba desarrollando tecnológicamente y el gran avance fue la persona jurídica. Una entelequia apropiada para la sociedad, una herramienta propedeútica adecuada para la sociedad dentro de un mundo de cambios en cámara lenta.

Sin dudas, existe una tendencia antropocéntrica,y todo tiene que ser a imagen y semejanza de los humanos. Las sociedades son personas que nacen, viven y mueren y, además, los animales nos contemplan mientras el derecho se desvela para calificarlos como personas "no humanas" (1).

Mientras tanto, la sociedad cambia, comienzan a desaparecer los íconos de nuestra sociedad, las cartas, los buzones, los teléfonos fijos, etc. Todo cambia.

El tema es de qué manera el derecho asimila los cambios o si simplemente opera dentro de un travestismo conceptual. Determinada institución o entidad es similar a otra categoría y en un extremo de simplificación, lejos de asignarle características específicas, naturaleza jurídica independiente o caracteres propios, la solución al estilo de contestador automático es colocarla en un plano similar a otro. Una fotocopia conceptual. De esa manera se van creando, o mejor estableciendo, nuevas categorías jurídicas, paraíso del "sui generis", con pretensiones de soberanía de género, sin que puedan adquirir personalidad propia (2).

II Ayer y hoy en la persona jurídica

En la historia, curiosamente en Roma, se concebía que eran personas algunos dioses como Apolo o Jupiter y en otras geografías se reconocía el carácter de personas a las plantas, animales y cosas inanimadas. Es como si en un viaje cósmico se acoplaran los actuales conceptos y los antiguos.

(*) Abogado. Doctor en Derecho. Profesor Titular de Derecho Internacional Público y de Derechos Humanos y Garantías, de la Facultad de Derecho de la Universidad de Buenos Aires. Autor de 15 libros y más de 100 publicaciones científicas. Premio UNESCO. Personalidad Destacada del Derecho declarado por la Legislatura de la Ciudad de Buenos Aires.

(1) Protección jurídica y respeto al animal: Una perspectiva a nivel de las constituciones de Europa y Latinoamérica.

ALTERINI, Atilio Aníbal, *¿Derechos de los animales?,* con mi afectuoso recuerdo.

(2) TRAVIESO, Juan Antonio, "Lenguaje y Derecho en los espacios marítimos", Jurisprudencia Argentina, Buenos Aires, nro 5287, 1982.

El derecho no se quedaba la zaga y también operaba confiriendo y sustrayendo derechos, como en el caso de los esclavos en cuanto a la capacidad de ejercicio de derechos de los mismos, diferente a la condición de ser humano. Proyectando a la actualidad, parecería que nada cambia en las relaciones de personas no humanas o robots.

Desde el derecho romano, el tema de la persona ocupa una gran parte de las reflexiones jurídicas, con diversas teorías que intentaban proporcionar una explicación racional.

Entre otras, la teoría de la ficción jurídica desarrollada en el siglo XIX, especialmente por Savigny. En esa teoría, parecería que se trata de un esquema antropocéntrico: el hombre es el único sujeto de derecho, por lo que la persona jurídica no tiene existencia real, sino que se trata de una ficción creada y utilizada por el hombre como una herramienta. El derecho en esos aspectos resulta producto de un relato brillante.

Cuando se advirtió que el mundo de las ficciones generaba dificultades, se delineó la teoría de la voluntad, con autores como von Gierke, G. del Vecchio y otros, que sostenían que la colectividad posee una voluntad independiente de sus miembros, anclando a las personas jurídicas en la voluntad social.

Más adelante se avanzó en la teoría del interés, de Von Ihering, luego la teoría de la institución de M. Hauriou y también la teoría de la construcción lógica de Hart, concebida como una "técnica del lenguaje jurídico".

El derecho está sembrado de teorías, y también se ha esbozado una posición formalista sobre la persona relacionada con el derecho. Desde ese punto de vista, persona física o jurídica, según Kelsen, es un haz de deberes y facultades jurídicas, un complejo de normas, o mejor, un conjunto de normas. En ese esquema en que el derecho es un sistema de normas, todo lo referente a la persona se relaciona inexorablemente con la normatividad.

En ese orden, la persona es un centro ideal de imputación de normas, representa una unidad de una pluralidad de normas dentro de una categoría jurídica formal. No es una realidad ni un hecho, es un conjunto de normas.

Por otra parte, en la tradición del derecho civil, recordamos a Alfredo Orgaz que consideraba que uno de los elementos esenciales de toda relación jurídica, sea de derecho privado o de derecho público, es la persona, es el sujeto del derecho que se contrapone al objeto. El sujeto y el objeto constituyen, por lo tanto, los dos presupuestos lógicos de toda relación jurídica (3).

Sin dudas, todo este formato y teorías van generando con plenitud la cosecha del universo del derecho que, con sus ficciones, es lo que es.

Por su parte, otros autores, como Ferrara, afirmaban que persona es "un concepto puramente formal que no implica ninguna relación de corporalidad o espiritualidad en el investido" y que es "una cualidad abstracta, ideal, proporcionada por la capacidad jurídica y no resultante de la individualidad corporal y psíquica" (4).

Pero hay otros puntos de vista.

Colin y Capitant consideraron que la persona solo se identificaba con los seres humanos. Estos son, para ellos, los sujetos del derecho, las personas propiamente dichas. Estas personas, "con dudosa exactitud llamadas físicas", son "las únicas verdaderas personas".

Pero esto no es todo. Hay otras teorías, que podríamos llamar, eclécticas, que sostienen que los autores que se adhieren a la tesis formalista y a la realista sobre la persona consideran solo un aspecto de una misma realidad. Una de ellas, apunta solo a los aspectos ético-jurídicos del problema y, por su parte, los formalistas, como expresamos, ponen en foco solo los as-

(3) Orgaz, Alfredo, *De Las Personas En Derecho Civil.* "Concepto de persona l. - Uno de los elementos esenciales de toda relación jurídica, tanto de derecho privado como de derecho público, es la persona, esto es, el sujeto del derecho. El elemento que se le contrapone el objeto. El sujeto y el objeto constituyen, por lo tanto, dos presupuestos lógicos de toda relación jurídica".

(4) Ferrara, Francesco, *Teoría de las personas jurídicas*, Editorial Reus, Madrid, 1929, ps. 318-319; *Teoría de las personas jurídicas*, 1ª ed., Comares, 2006.

pectos normativos, dejando de lado la realidad existencial.

Los autores concluyen que es necesario armonizar las teorías y en ese punto de vista se hallan Spota y Orgaz. Sin dudas, ese concepto nos conduce a ampliar la denominación de persona a otros entes, sujetos o entidades.

Allí el tema se enfoca a aplicar una concepción integral de la persona que refleje la interacción dinámica entre vida humana social, valores y normas jurídicas, acentuando los elementos axiológicos.

Otro planteo es el referente al derecho internacional de los derechos humanos y ha establecido el llamado principio " pro hominem" que, actualmente y justificadamente, se lo denomina con precisión principio " pro persona", que opera como un solucionador de conflictos, acentuando los derechos de la persona.

De esta manera, se advierte que el concepto de persona opera, al estilo Newton, como un haz de luz en un prisma que ofrece múltiples enfoques normativos, eclécticos, axiológicos, etcétera.

Lo interesante es que el concepto de persona se ha fertilizado y transportado a todos los sistemas jurídicos y en la actualidad pugna por inundar y sobrevolar distintas realidades relacionadas con la tecnología (5).

El tema, ahora es si es posible reconocerle personalidad jurídica a un robot dotado de inteligencia artificial.

La cuestión de la personalidad jurídica quizás es la menos conflictiva. El problema es determinar la capacidad de obrar, esto es, definir qué actos pueden o no hacer las personas jurídicas en este paisaje "*border line*". Más allá de lo expuesto, la cuestión es también qué es lo que pueden hacer los robots con el auxilio de la inteligencia artificial en ese límite cada día más borroso con lo humano.

Así pues, esa cuestión requiere un serio debate, ya que con la robótica y la inteligencia artificial aparece una nueva dimensión. Además, hay que verificar si hay una o varias personas responsables de la gestión, así como qué facultades tienen esas personas y qué requisitos hay que reunir para ser persona jurídica, como lo analizaremos más adelante.

El tema es, ahora, de qué manera se construye la personalidad jurídica de los robots y, en ese sentido, ya se está tratando de un nuevo derecho: el derecho civil de los robots (6).

El dilema que se plantea hoy, ante las actividades que van realizando los robots y los programas de inteligencia artificial, no es analizar los límites físicos, sino, en especial, los jurídicos. Ese es el tema. Pero, previamente, hay que establecer el marco de acción.

III. Hacia un nuevo mundo con más y diferentes personas. Post humanismo y Transhumanismo en el mundo del derecho

1. La nueva modernidad líquida

En la actualidad, el derecho se presenta como una obra de ingeniería y de arquitectura. Octavio Paz decía que la arquitectura es el testigo menos sobornable de la historia; seguramente respetando a Aristóteles, quien afirmaba que cuando se construye bien, se llega a ser un buen arquitecto e ingenioso poeta como Gaudí y su Catedral de la Sagrada Familia. Además, cuestiones como la globalización, la regionalización y los nuevos esquemas del mundo están obstruyendo las reflexiones, dado que resulta inevitable hacer referencia al nuevo escenario.

Estos tres conceptos plantean un enfoque diferente en el derecho y quizás el gran tema táctico es lo que podríamos denominar el cam-

(5) Kelsen, Hans, *La teoría pura del derecho*, 2ª ed., Losada, Buenos Aires, 1946, p. 83; Borda, Guillermo A., *Tratado de Derecho Civil Argentino*, Abeledo Perrot, Buenos Aires, 1955, ps. 205-207;Ferrara, Francesco, *Teoría de las personas jurídicas*, cit., p. 332. Dentro de los autores que aceptan la teoría formalista sobre la persona —aparte de Ferrara y Kelsen— podemos citar a Lehman, Von Thur, Josserand, Michoud, los Mazeaud, De Diego, De Cupis, Di Semo, Gangi, Rotondi, Barassi, Bevilacqua, Salvat, entre otros. Todos ellos, o casi todos, desarrollan sus trabajos jurídicos en la primera mitad del siglo XX o en los últimos años del siglo XIX.

(6) *http://www.europarl.europa.eu/committees/fr/supporting-analyses-search.html.*

bio del tiempo verbal en el pensamiento del yo soberano al nosotros inmersos en un mundo tecnificado con redes sociales.

En ese escenario, la tecnología ha producido importantes cambios en el derecho.

Así, en la actualidad, en vez de disparar balas se lanzan ráfagas de metralla virtuales y continuas en los medios de comunicación a través de redes sociales. Para ser militante global solo hace falta empuñar un mouse con Internet y banda ancha y si se tiene *big data*, mejor.

Zigmunt Bauman ha marcado la existencia de un nuevo mundo, el de la modernidad líquida, frágil, desgarrada, heterodoxa, en contraposición con la modernidad sólida del siglo XX, que vivimos todos nosostros (7).

Lo mismo ha sucedido con el diseño de sociedad que cambió tan profundamente, ya que en quinientos años pasamos a descubrir que la tierra no era redonda, pasó a ser plana luego de internet y otros factores (8).

Se trata de una nueva sociedad que se resiste a ser como era hace cincuenta años e incluso presiona para producir innovaciones, dentro de un nuevo esquema, con relaciones cada día más disruptivas en este modelo de sociedad líquida que nos propone Bauman en contraposición con la sociedad sólida, predictible, a la que estábamos acostumbrados, con cambios que se iban produciendo al ritmo de un reloj de arena.

Una sociedad rígida que se contrapone a la nueva, que incluso plantea hasta un nuevo lenguaje con niños nativos digitales, ya adolescentes y algo más, que miran con perplejidad aun los cambios que no alcanzan a entender y el nuevo celular con una manual desactualizado al mes de comprarlo.

El nuevo modelo social que se avecina va a producir cambios de gran calado respecto a la sociedad industrial, que van a influir no solo en la vida cotidiana, sino también en las estructuras políticas, económicas y sociales. Algunos conceptos firmemente arraigados, como el de soberanía nacional, sometimiento al principio de legalidad, sistemas de control y la propia democracia representativa van a tener que ser revisados ante esta nueva realidad.

En ese mundo, diferente y cambiante se abren nuevas y diferentes ventanas, posibilidades y obstáculos. En ese mundo, la inteligencia siempre ponderada y natural, patrimonio de los genios y dotados, comienza a ser puesta en pugna con otra inteligencia no tan sutil ni emocional,: la inteligencia artificial (en adelante IA).

En ese espacio tecnológico, habitan nuevos sujetos o personas que los humanos se esfuerzan por "empoderar", utilizando expresión de moda, y hacerlos cada vez más a su imagen y semejanza. En ese espacio tecnológico, cada día hay más personas, en el mismo mundo y además con diferentes personas en el borde de lo humano y técnico.

En ese mundo, además la tecnología es el modelo de la sociedad, conquistador y globalizador.

2. El nuevo modelo tecnológico. La inteligencia artificial IA. SOS: los robots fuera de control

Desde el punto de vista científico, se viene analizando el proceso de instalación de la tecnología. Los autores se refieren a seis fases para la puesta en marcha o implantación de una tecnología: iniciación, adopción, adaptación, aceptación, rutinización e infusión.

Esos procesos habituales en la tecnología no existen o son embrionarios en el derecho.

Lo que sucede es que el proceso de cambio se presentó en todas las materias del derecho. Por ejemplo, en el derecho internacional, demandó más 300 años. No hubo mayores cambios hasta hace pocos años, después de la Segunda Guerra Mundial, cuando hizo irrupción el Derecho Internacional de los Derechos Humanos luego de la Carta de la ONU de 1945 y la Declaración de Derechos Humanos de 1948.

Pero, mientras el derecho transcurre y se discute sobre la responsabilidad en las paredes hu-

(7) Bauman, Zygmunt, *Maldad Líquida*, Paidós; *Amor Líquido*, Paidós; *Vida Líquida,* Austral; *Tiempos Líquidos*, Tusquets; *Generación Líquida*.

(8) Friedman, Thomas, *La tierra es plana Breve historia del mundo globalizado del s. XXI*, Martínez Roca, 2005.

medecidas y desmoronadas de las normas, códigos y resoluciones, en la era digital casi todo es *big data*.

Todos los datos de las personas se hallan listos para explorar y ser explotados con finalidades diversas. Se trata de un fenómeno que opera con cantidades enormes de datos, con finalidades imposibles de mensurar.

Un modelo 4.0 de sociedad que elabora *fake news* (9) y en el colmo proyecta nuevas monedas, como Facebook que propone la Libra (10).

En ese diseño de sociedad, un grupo de científicos y expertos del mundo de la tecnología crearon en conjunto una comunicación para que personas comunes y corrientes presten una mayor atención ante la maravilla que parece la *inteligencia artificial*. Dicho grupo, entre los que se encuentran nada menos que Stephen Hawking**,** Elon Musk, Verno Vinge y otros destacados expertos en ciencia y tecnología, elaboró el documento denominado *Research Priorities for Robust and Beneficial Artificial Intelligence: an Open Letter* (Carta Abierta: Prioridades de Investigación para una Inteligencia Artificial fuerte y beneficiosa).

El documento toma en cuenta décadas de investigación sobre inteligencia artificial y, entre las principales advertencias, se refiere a la posibilidad de que, en un ambiente no controlado en forma adecuada, los sistemas de inteligencia artificial podrían tener comportamientos no deseados e incluso dañinos.

La comunidad muestra así la preocupación ante una posible *independencia de inteligencia artificial* capaz de que pueda tomar vida propia y superar la que ha supuesto el hombre.

En ese punto de vista, quienes hoy estamos a cargo de estos dispositivos perderíamos el control sobre las máquinas y estas podrían actuar en contra nuestra. Según el citado texto, las investigaciones deberían enfocarse en lograr que quienes trabajan en estas cuestiones tomen medidas de seguridad ante una rebelión robótica en caso de problemas. Suena extraña la idea de una rebelión robótica, pero es el modo de asignarle personalidad a través del peligro que generarían.

Google es quizá la empresa que más apuesta por el desarrollo de Inteligencia Artificial a través de su máquina *Deep Mind*, la que ya nos mostró varios avances impresionantes, pero este sistema también tiene su lado oscuro, tal como pudieron comprobar en una reciente prueba.

Deep Mind es capaz de aprender por sí misma y hasta imitar de forma casi perfecta a los humanos, tanto que, al notar que va perdiendo en un juego, se enoja y *se torna violenta*, lo que nos hace temer por las reacciones que podrían tener los robots con IA.

Pero no todo fue fácil.

Desde los años 80 y 90 empezaron a circular en el mundo intelectual y académico occidental términos como deconstrucción, posmodernismo, poscolonialismo, que cuestionaban los fundamentos epistemológicos de la modernidad y del orden mundial establecido y proclamaban el fin de las utopías y de las ideologías totalizantes, así como un cambio radical en la cultura. Este espacio comienza a ser colonizado por los robots.

Una nueva era, un nuevo siglo que se caracteriza por la velocidad y el ciberespacio. El siglo del avance de las periferias frente a las metrópolis, el de la revolución digital.

Se trata del siglo XXI, que dejaba atrás el humanismo tradicional para dar paso a otras concepciones de lo humano y a otras subjetividades.

Imaginemos estos cambios ante el concepto de persona jurídica, cristalizado en las bibliotecas jurídicas, mientras el mundo iba cambiando a toda velocidad. Lo cierto es que se produjo una asincronía, un desfasaje que implosiona los conceptos. Lo que sucede, es, como decía Paul Valery, que el futuro ya no es lo que era.

Todo esto sucede mientras se proyecta en nuestros Ipad la imagen de Metrópolis de Fritz

(9) House of Commons, Digital, Culture, Media and Sport Committee "Disinformation and 'fake news': Final Report", Eighth Report of Session 2017-19, Ordered by the House of Commons, to be printed 14 February 2019.

(10) "La moneda de Facebook ya genera suspicacias", La Nación, 22 de junio de 2019.

Lang de 1927 con los rascacielos y el robot en primer plano con el inicio de la ciencia ficción.

En efecto, los humanismos del siglo XX que tenían como base epistemológica el hombre como medida de todas las cosas ya no se adecuaban a las nuevas sociedades de la información, de la velocidad, de la ciencia y de la tecnología.

El filósofo que encendió la polémica fue Peter Slodertdijk, generando la reflexión filosófica sobre el posthumanismo que al principio fue muy elogiada por el mismo Jürgen Habermas, antes de entrar en el debate a raíz del libro del primero, llamado *Normas para el parque humano*.

La obra filosófica de Sloterdijk, posterior al libro de la polémica, está constituida principalmente por *Esferas I, Esferas II* y *Esferas III*, en las cuales hace un planteamiento muy original sobre las nuevas formas de relaciones humanas y las transformaciones del espacio íntimo, privado y de los espacios públicos a partir de la revolución digital.

Siempre es de utilidad poner a prueba pensamientos contra fácticos, como dirían los psicólogos. F. Scott Fitzgerald dijo que la prueba de la inteligencia de primer nivel es la capacidad de tener dos pensamientos contradictorios al mismo tiempo. Vamos a comprobar si esta afirmación es verdadera o falsa.

Lo cierto es que el hombre posmoderno y posthumano ya no es el sujeto autónomo de la Modernidad, dueño de una voluntad y convencido de que la razón lo distinguía porque era una cualidad exclusiva de nuestra especie. El hombre posmoderno y posthumano sabe, gracias a la cibernética y la revolución tecnológica, que la razón no le es exclusiva, pues esa razón puede ser copiada y reproducida fuera de su cuerpo por cualquier máquina inteligente. La imagen del cerebro como una computadora que es herencia de la cibernética muestra con claridad la desaparición del hombre, que estaba en el centro del humanismo moderno. Esta es una característica del sujeto posmoderno: la transferencia de la razón fuera del cuerpo humano e incluso su superación, pues algunas máquinas pueden superar la racionalidad humana en el procesamiento de datos.

La reflexión filosófica de esta nueva era tiene representantes importantes, filósofos contemporáneos que han debatido los fundamentos y límites de la posmodernidad como Derrida, Deleuze, Baudrillard, entre otros que han ido descentrando la idea de un sujeto autónomo racional.

Sin embargo, quien ha utilizado el término "posthumanismo" para hablar de una nueva época y dar por finalizada la era del humanismo tradicional es el filósofo citado Peter Sloderdijk. La referencia a él y a la polémica que sostuvo a final del año 1999 con Jürgen Habermas es una cita obligada al hablar sobre el pensamiento del posthumanismo.

A raíz de la conferencia que impartió Sloterdijk titulada "Normas para el parque humano. Crítica de la carta del humanismo de Heidegger" y a las interpretaciones que varios filósofos alemanes —incluyendo Habermas— hicieron a su contenido, se desató una polémica en Alemania que dio una gran popularidad a Sloterdijk. En ese enfrentamiento intelectual entre ambos pensadores, se formularon mutuas acusaciones morales e intelectuales. Los principales cuestionamientos que se hicieron a lo expuesto por Sloterdijk era que parecía defender y apoyar la manipulación genética de la descendencia a través de una antropotécnica.

Para Sloterdijk, el "hombre" del humanismo es un pensador autónomo y racional, capaz de mejorarse a sí mismo a través de la educación y la auto-reflexión, sin perjuicio de que los hechos parecerían indicar lo contrario. Lo cierto es que parecería que la cultura humanista ha fracasado y que el potencial barbárico de la civilización está creciendo más cada día. Los instrumentos de la educación, el humanismo como ideal civilizatorio, no han dado los resultados esperados y, por tanto, sostienen los autores, la ingeniería genética podría ser el camino para mejorar el ser humano. En ese panorama, también se presentan los robots y su papel en el futuro cercano.

3. El Posthumanismo. Máquinas que superan la razón humana: androides, robots y cyborgs

Como expresamos, las IA generan nuevos razonamientos con relación a los robots. El tema

no es solo el debate acerca de su eventual personalidad jurídica, sino la hipótesis de su independencia y su eventual rebelión que, al igual que Espartaco, se rebela a sus amos.

Hace unos años, *Isaac Asimov* (1920–1992), considerado uno de los grandes escritores de ciencia ficción de su época, postuló tres leyes que, de ser respetadas, evitarían un levantamiento de robots. Aunque conocidas por todos, las reproduciremos.

Son las siguientes:

Ley 1: Un robot no puede dañar a un ser humano o, a través de la inacción, permitir que un ser humano sufra daños.

Ley 2: Un robot debe obedecer las órdenes que le dan los seres humanos, excepto cuando tales órdenes entren en conflicto con la primera ley.

Ley 3: Un robot debe proteger su propia existencia siempre que dicha protección no entre en conflicto con la primera o la segunda ley.

En realidad, es evidente que Asimov no previó que los robots podían llegar a rebelarse. Es como los robots en el mundo de Alicia, la del país de las maravillas.

La transferencia de la razón fuera del cuerpo humano (e incluso su superación, pues algunas máquinas pueden superar la racionalidad humana en el procesamiento de datos), es una característica de un mundo donde lo humano convive al mismo nivel con los agentes no humanos y se borran las fronteras entre estos, pues ambos son valorados por su capacidad de recibir y procesar información.

Así, se desmantela el andamiaje filosófico que caracteriza la "identidad humana" como una identidad singular, separada del mundo de los objetos y en posición jerárquica privilegiada dentro de la sociedad. Por tanto, esto trae como consecuencia no solo cambios en la noción de "lo humano", sino también reformulaciones del entorno social porque ya no estamos frente a una sociedad constituida solamente por seres humanos, sino que los agentes no humanos adquieren cada vez mayor relevancia y la interacción entre humanos y no humanos transforma nuestras ideas de la vida en sociedad. La pregunta que se plantea es qué diría Nietzsche en su obra *Humanos demasiado humanos*, o quizás debería actualizarse el título por *Robots y humanos, demasiado humanos*.

A partir de esta etapa, consideramos que hay que establecer algunas definiciones.

Según la ciencia popular, hay que poner en claro algunas diferencias entre androide, robot y *cyborg*.

> Androide es el nombre que se le da a un robot antropomorfo, es decir, que tiene forma o apariencia humana, y además imita algunos aspectos de su conducta de manera autónoma. La palabra androide posee un origen etimológico griego, al estar constituido por andro (hombre) y eides (forma).
>
> Por otra parte, un robot es una máquina o ingenio electrónico programable, capaz de manipular objetos y realizar operaciones antes reservadas solo a las personas. El robot humanoide es aquel que se limita simplemente a imitar los actos y gestos de un controlador humano, por lo que no es un verdadero androide, propiamente dicho.
>
> Con relación a "cyborg", es una palabra que se forma a partir de las palabras inglesas Cyber(netics) organism (organismo cibernético) y se utiliza para designar una criatura medio orgánica y medio mecánica, generalmente con la intención de mejorar las capacidades del organismo utilizando tecnología artificial (11).

Para Sloterdijk (2008), el humanismo tradicional, basado en la cultura del libro y en la ilusión de que un canon de lecturas y unas técnicas pedagógicas podrían civilizar al hombre, ha fracasado. En este siglo de la velocidad, de las tecnologías de la información, de las biotecnologías y la globalización cultural, "la coexistencia humana se ha instaurado sobre fundamentos nuevos".

(11) *http://www.cienciapopular.com/n/Tecnologia.*

Actualmente, la socialización de los humanos está en manos de los medios de información y las nuevas tecnologías.

Es el siglo de la velocidad y del cambio, mientras Sloterdijk se cuestiona: ¿por qué no usar otros medios para promover esa domesticación que tanto se buscó y no se logró con el humanismo letrado? Para él, el uso de las biotecnologías es parte de las antropotécnicas o conjunto de técnicas desarrolladas para modificar el comportamiento humano.

Si hay hombre es porque una tecnología lo ha hecho evolucionar a partir de lo pre-humano. Ella es la verdadera productora de seres humanos o el plano sobre el cual puede haberlos. De modo que los seres humanos no se encuentran con nada nuevo cuando se exponen a sí mismos a la subsiguiente creación y manipulación y no hacen nada perverso si se cambian a sí mismos autotecnológicamente, siempre y cuando tales intervenciones y asistencia ocurran en un nivel suficientemente alto de conocimiento de la naturaleza biológica y social del hombre y se hagan efectivos como coproducciones auténticas, inteligentes y nuevas en trabajo con el potencial evolutivo. (Sloterdijk, 2006, p.14).

Así pues, para Sloterdijk, el ser humano ha tenido siempre que autotransformarse para preservar su existencia y es perfectamente lógico que surjan nuevas antropotécnicas, una de las cuales podría ser la robótica.

Desde la posición contraria, Francis Fukuyama (2002) adopta una posición de resistencia frente a la aplicación de las biotecnologías y propone defender la "identidad humana" y salvaguardar la naturaleza humana cuando dice que "... la amenaza más significativa planteada por la biotecnología es la posibilidad de que ella alterará la naturaleza humana y nos llevará a un estado posthumano de la historia. Esto es importante, yo diría, porque la naturaleza humana existe, es un concepto significativo y nos ha proporcionado una continuidad estable a nuestra experiencia como especie". (Fukuyama, 2002, p. 7) y, finalmente, el autor citado considera que el posthumanismo representa la más grande amenaza contra los cimientos de la sociedad humana. Esta posición de Fukuyama se pone en línea con la ingeniería genética que opera cortando el ADN y generando un nuevo ser humano.

Por supuesto, la antropotécnica pone en jaque un modelo de civilización y, por supuesto, impacta en el mundo del derecho.

Como se advierte, hay posiciones diferentes adaptadas para los distintos puntos de vista.

IV. Los robots en el mundo del derecho

1. Los robots, nuevos protagonistas

Ahora, veamos los resultados de algunas investigaciones que instalan a los robots en la realidad y en el marco de las relaciones humanas, en todos los ámbitos de la vida, más allá y dentro del derecho.

Primero veamos en la literatura. Hace pocos días se ha publicado un artículo en el que los robots reinterpretaban a Shakespeare. ¿Robots literarios? (12)

En segundo lugar, veamos en la tecnología del mañana hoy en las relaciones de los robots de ellos entre sí y con nosotros los humanos..

Facebook, en la sección de desarrollo de inteligencia artificial (*Facebook artificial Intelligence researchers*), *creó un sistema* dedicado para observar el modo de interactuar de los robots en las negociaciones.

Lo cierto es que los dos «*bots*» (programa informático que imita el comportamiento humano), llamados Bob y Alice, usaban palabras aleatorias y sin sentido, por ello l*os investigadores pensaron* en un primer momento que el sistema IA estaba sufriendo un fallo. Sin embargo, tras un análisis, se percataron que en esas palabras había un patrón, por lo que los «bots» habían creado su propio lenguaje porque habían considerado que de esta manera era mucho más directo que el inglés. Ante la dificultad de la comunicación entre el sistema y el ser humano, Facebook ha decidido apagar el sistema antes de perder por completo el control.

(12) Corso, Pablo, "Los robots sueñan con tener la inspiración de Shakespeare", La Nación, 15 de julio de 2019.

De esta manera, los resultados de las pruebas acreditaron que los «*bots*» estaban conversando en un lenguaje extraño y aparentemente erróneo. Sin embargo, no se trataba de un error, ya que el sistema había creado su propio idioma. Ante este tipo de interacción por cuenta propia, Facebook decidió desactivarlos. ¿Temor o precaución?

El problema para un sistema de IA es que, si decide por su cuenta ignorar el idioma mediante e*l cual ha sido programado*, supone una dificultad para el desarrollo de redes neuronales y la posterior tecnología que su fabricación pueda suponer.

En ese orden de ideas, se ha considerado, con razón que "Si la IA realmente diera vida a los personajes, ¿no tendríamos que preguntarnos por sus derechos", tal como sugiere entre otros el filósofo Peter Sloterdijk?".

Microsoft no se hizo tantos cuestionamientos cuando desconectó a Tay el 24 de marzo de 2016, apenas 16 horas después de haberlo subido a las redes sociales. La cuestión es que el robot se comenzó a mostrar entusiasmado por conocer a personas reales.

En ese momento, todo se complicó. Tay empezó a tuitear que odiaba a los judíos, que Hitler tenía razón, que Barack Obama era un mono, que México tenía que pagar el muro y que las feministas debían arder en el infierno. Doloroso, pero lógico: había aprendido de las ideas y palabras discriminadoras de sus interlocutores.

Sus creadores estaban furiosos, además, con una respuesta en especial. Cuando le preguntaron qué consola de videojuegos prefería, Tay eligió a los video juegos de la competencia.

Por ello, cabe afirmar que los robots y los sistemas de inteligencia artificial son uno de los grandes inventos verdaderamente disruptivos del entorno digital y constituyen, sin duda, un vector de cambio vertiginoso de nuestras sociedades, que apenas se ha comenzado a percibir y cuya tecnología no se puede explicar. Su interacción es a veces agradable y otras no tanto.

Lo que une a todos estos artefactos es la característica de que tales sistemas presentan cierto grado de autonomía en su funcionamiento, de «impredecibilidad», por decirlo de alguna manera, y también cuentan con la capacidad de causar daño físico, lo que abre una nueva etapa en la interacción entre los seres humanos y la tecnología (13).

2. Los robots en el derecho. Hacia la regulación jurídica

Ahora, entra al escenario el derecho.

Por supuesto que el derecho es el derecho de todos los días con toda su historia. El tema es incorporar estas nuevas estructuras tecnológicas en el mundo del derecho. De alguna manera, adelantamos que el tema es encorsetarlos y sujetarlos a un orden, el de las normas.

No es simple instaurar estructuras super tecnológicas y actuales en el mundo clásico jurídico. Adelantamos que se trata de una tarea difícil, pero no imposible.

De esta manera, para afrontar los retos que traerán los nuevos ejemplares de robots a causa de la cuarta revolución industrial, los europarlamentarios han llegado a la conclusión de que es necesario elaborar un estatus legal de la "persona electrónica". Los robots son una realidad en expansión y es necesario, según los científicos, abordar la responsabilidad, la seguridad y la gestión de riesgos relacionados con su actividad.

La Comisión de Asuntos Jurídicos del Parlamento Europeo (14) ha aprobado un informe, cuyo objetivo es regular la inteligencia artificial, crear un registro de robots e impulsar una agencia dedicada a este asunto.

La propuesta solicita a la Comisión Europea la creación de un estatuto jurídico específico para la IA y para los robots de automatización de tareas, la creación de un fondo general para todos los autónomos inteligentes o bien crear un fondo individual para cada definición y clasificación de los «robots inteligentes»

(13) *http://www.europarl.europa.eu/committees/fr/supporting-analyses-search.html.*

(14) A8-0005/2017 27.1.2017 INFORME con recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica (2015/2103(INL)).

Así pues, debe establecerse una definición europea común de robots autónomos «inteligentes», cuando proceda, incluidas las definiciones de sus subcategorías, teniendo en cuenta las siguientes características:

– la capacidad de adquirir autonomía mediante sensores y/o mediante el intercambio de datos con su entorno (interconectividad) y el análisis de dichos datos;

– la capacidad de aprender a través de la experiencia y la interacción;

– la forma del soporte físico del robot;

– la capacidad de adaptar su comportamiento y acciones al entorno.

Ahora estamos en presencia de la ficción que se hace realidad en el mundo del derecho.

Reflexionemos desde los personajes de la ficción como Frankenstein, creado magistralmente por Mary Shelley, hasta el mito clásico de Pigmalión, pasando por el Golem de Praga o el robot de Karel Čapek —que fue quien acuñó el término—.

Con esos antecedentes de la ficción, los seres humanos hemos fantaseado siempre con la posibilidad de construir máquinas inteligentes, sobre todo androides con características humanas. Volvamos a recordar el célebre film Metropolis de Friz Lang, que representa una prueba de los expuesto hace casi un siglo (15).

El tema es, entonces, asimilar que estamos en vista de una nueva era en la que robots, *bots*, androides y otras formas de inteligencia artificial protagonizan una revolución industrial, —que afectara trasversalmente a la sociedad—, en especial en el mundo del trabajo y, por tanto "resulta de vital importancia que el legislador pondere las consecuencias jurídicas y éticas, sin obstaculizar con ello la innovación".

La cuestión a analizar es que, cronológicamente, entre 2010 y 2014, las ventas de robots aumentaron un 17% cada año, e incluso en 2014 las ventas registraron el mayor incremento anual: un 29 %.

Ahora, los principales motores de este crecimiento son los proveedores de componentes de automotrices y la industria electrónica y eléctrica que, a lo largo del último decenio, han triplicado las solicitudes anuales de patentes en el sector de la tecnología robótica.

Estos cambios en materia de robots van a impactar no solo en el modo de vida, sino también en los niveles de eficiencia, ahorro y seguridad y en la calidad de los servicios en la producción y el comercio, el transporte, la asistencia sanitaria, las operaciones de salvamento, la educación y la agricultura. Ni hablar de la medicina y su progreso por medio de la robótica y en especial en la capacidad de pensar y tomar decisiones.

El panorama de las actividades, con la presencia de los robots adquiere caracteres especiales, en materia de Robots asistenciales con el desarrollo de robots médicos, utilizados en rehabilitación e intervenciones en el cuerpo humano.

También, otro aspecto que se abre ante los robots son las consecuencias en *materia fiscal*. En esta cuestión, la Comisión propone que las empresas que hayan utilizado robots para procesos industriales para garantizarse menores costes en recursos humanos deberán declarar los ahorros en contribuciones a la seguridad social a efectos de compensar los cambios laborales producidos.

Curiosamente, el tema es tan importante que ahora se están planteando "robots imponibles".

3. Robots otra vez fuera de control. ¿Quién se responsabiliza por los daños? Otros temas.

Una vez planteado el aspecto regulatorio general, ahora se abre el campo específico del derecho en algunas de sus ramas.

Así pues, otro tema a tener en cuenta es el vinculado con la responsabilidad jurídica de los robots fuera de control y emancipados.

La unión Europea considera que una posible solución a la complejidad de la asignación de responsabilidad por los daños y perjuicios causados por robots cada vez más autónomos podría ser el establecimiento de un régimen de seguro obligatorio.

(15) *https://www.youtube.com/watch?v=xi1cGGCJKDg.*

Junto con la responsabilidad ante la situación de una "personalidad electrónica" se plantea, además de la responsabilidad, el tema de la privacidad, del robot que interactúa en nuestras casas.

El tema se presenta con Alexa, que apareció en noviembre de 2014 cuando Amazon lanzó el Echo, un elegante altavoz casero de forma cilíndrica con soporte para inteligencia artificial al que denominó Alexa, que rápidamente se impuso en muchos hogares. La cuestión es que Alexa interactúa, pero también escucha las conversaciones privadas. Eso es un gran problema.

En otro sector aparece *Robear*, un gigante oso blanco robótico que es por el momento un prototipo de autómata japonés para ayudar a los enfermeros a levantar pacientes de la cama y sentarlos en su silla de ruedas. *Pepper*, otro de esos simpáticos robots sociales, ya trata incluso de leer nuestras emociones. Pero, por muy bien que nos caigan estos robots, si se instalan en nuestros hogares podrían llegar a saber demasiado sobre nuestras vidas.

Uno de los planteamientos que incluye el proyecto de *Reglamento Europeo de Protección de Datos* es la *'privacy by design'*, la privacidad por diseño. Algunos autores consideran que se trata de "construir un dispositivo conforme a la normativa de protección de datos y no construir un dispositivo y luego pensar cómo podemos hacer para que el dispositivo cumpla, sino que el propio dispositivo vele por proteger la privacidad del usuario".

En el caso de los robots cuidadores, la privacidad cobra especial importancia. "Ese robot sabe perfectamente qué medicamentos estoy tomando o si estoy mejorando, quién viene a mi casa a verme... se considera que se trata de un tema polémico", porque "La invasión de la intimidad de estos aparatos es mucho más alta y hay que vigilarla con atención. Pues no es suficiente que alegre e inconcientemente aceptemos términos y condiciones con un click que ponen en jaque nuestra privacidad.

Por otra parte, en Europa y Estados Unidos de América ya comienzan a aparecer los hipotéticos problemas legales que planteamos ante la aparición de Alexa.

Por supuesto que allí aparecen de nuevo las leyes de la robótica de Asimov que ya expusimos, porque esas famosas leyes siguen formando parte del terreno de la ciencia ficción, pero nadie se ha puesto a elaborar otras que se apliquen a los casos reales.

Los cierto es que, por el momento, no hay normativa específica en Europa o Estados Unidos que regule la responsabilidad de los robots, aunque alguien va a tener que asumir las consecuencias de sus actos.

La primera idea que ha surgido es usar reglas conocidas y, por tanto, aplicar el mismo régimen que a un producto defectuoso. En esa simplificación totalizadora no hay diferencia entre un robot, una antena o unos zapatos. De esta manera, pues, se ha considerado que, si el robot falla, se aplica la misma normativa de responsabilidad del fabricante. Si el robot causa un daño al usuario, es responsabilidad del fabricante.

Hasta aquí todo es simple y habitual en el derecho. El tema se presentará cuando o un robot decida comprar pastillas de éxtasis, cocaína o marihuana porque sus programadores le han dejado solo en el mercado de la internet profunda. Aclaramos que ese experimento *ya se ha llevado a cabo*, como parte de un proyecto calificado de artístico.

Por supuesto que todo el progreso tecnológico es apasionante hasta que un *coche autónomo* se estrelle contra otro para evitar atropellar a un peatón, o un robot enfermero controle *hasta nuestro azúcar en sangre* y se equivoque.

En esos casos, habrá que replantearse las implicaciones legales de los robots.

El tema es que todo funcionaba bien hasta que los robots comenzaron a independizarse. Todo andaba bien mientras se consideraba que eran máquinas tontas, dedicadas a ejecutar cosas para las que estaban programadas.

Pero es el caso que han dejado de ser máquinas tontas y cada vez, como lo señalamos, realizan actividades más "racionales".

La primera pregunta que se plantea es acerca de la responsabilidad de los robots y, en realidad, quién es responsable de sus acciones

presuntamente dañosas. Esto supone, pues, las consecuencias jurídicas del accionar de los robots.

Volvamos atrás y veamos las aristas que se presentan ante la programación del robot drogadicto que abre un conflicto jurídico e incluso al margen de la ley.

Lo cierto es que sus creadores sabían que estaban haciendo algo ilícito, por lo que podrían ser considerados responsables de la adquisición de sustancias ilegales. Una situación clara que al ser ejecutada por un robot se hace confusa.

Se ha considerado que la persona que utiliza o ha diseñado un *'bot'* que termina comprando algo ilegal o que, por caso, emite una *aparente amenaza de muerte*, se presenta dilemática.

En el caso expuesto, por un lado se infringió la ley, pero al analizar la intención de cometer un delito, podría estar ausente, toda vez que cabe considerar que tal comportamiento no fue anticipado.

Se ha dicho que el robot no es responsable: "es solo una herramienta que está siendo utilizada con malos propósitos", como lo ha considerado Andrea Bertolini, uno de los autores del *informe Robolaw* financiado por la Comisión Europea. Recordemos que este proyecto debate las implicaciones éticas y legales de los robots y proporciona una serie de reglas generales para una posible futura regulación (16).

Así, se ha considerado en los trabajos citados que los autores de Robolaw no creen que haya que adoptar una definición única de *robot* (un término que *proviene de la ciencia ficción* y que no creen sea útil desde una perspectiva jurídica) y abogan por un estudio caso por caso. "No puedes tratar las prótesis robóticas como los coches inteligentes, son muy diferentes los unos de los otros, son problemas diferentes con soluciones diferentes", asegura Bertolini, investigador de Pisa.

La cuestión se presentará cuando la responsabilidad de un accidente de tránsito deje de ser del conductor porque los coches autónomos circulen por las carreteras, ¿quién será el responsable? ¿El fabricante o el desarrollador del *'software'*? ¿Y si un humano ha modificado las características del *'software'*, ya sea un ciberatacante o incluso el propietario?

Se ha dicho que "Generalmente, la compañía que desarrolla el producto es responsable cuando algo se vuelve inseguro, pero el tema se presenta cuando se diluya la responsabilidad en el caso en que una empresa fabrica el robot y otra programa las aplicaciones y el software".

Por eso es que se deberá prever que, previo a que las aseguradoras acepten los nuevos retos del vehículo sin conductor, habrá que establecer la seguridad que se va a exigir al fabricante para que ese coche pueda circular.

Por eso es que se ha señalado por Bertolini que "Una solución es crear nuevos estándares tecnológicos que aseguren mejor que el producto es seguro antes de venderlo en el mercado. Necesitaríamos un mejor sistema que no necesite la directiva de responsabilidad de producto defectuoso, sino reglas alternativas que no castiguen tanto al productor del dispositivo" a los efectos de no afectar el desarrollo de la tecnología.

Por otra parte, el informe Robolaw recoge para estos casos la eventual creación de una **"***personalidad electrónica***"** para los robots. Se ha dicho que hay diferentes sectores de responsabilidad: el de los fabricantes, el de los dueños de los robots, como en el caso de las mascotas.

En un tercer escalón, de manera audaz, se conferiría a los robots cierta responsabilidad no jurídica, para intentar que respondan por los daños causados.

Otra de las cuestiones que se plantean es el caso hipotético de que un robot destinado a la seguridad fuera capaz de tomar sus propias decisiones y optara por disparar a una persona. En ese caso, ¿cuáles serían las alternativas antes de encarcelar al robot? ¿Quién es el responsable? ¿El fabricante, la empresa de seguridad propietaria del robot, el propio robot?

(16) *http://replicantelegal.com/robolaw-i-orientaciones-para-regular-los-robots-en-europa/ www.eldiario.es/hojaderouter/tecnologia/robot-ciborg-inteligencia_artificial-derecho-leyes_0_385661559.html.*

Muchos dilemas y pocas soluciones.

Por su parte, el informe Robolaw plantea dotar a los robots de personalidad electrónica cuando sean autónomos, una suerte de responsabilidad *'ad hoc'* a esos robots capaces de aprender por sí mismos y tomar decisiones y se propone dividir la responsabilidad en personalidad mecánica o personalidad robótica y, al tener ciertas capacidades, se podría juzgar a ese robot y, en caso extremo, destruirlo.

4. Normas para cyborgs

Otro tema aún no regulado es acerca de las modificaciones del cuerpo humano en el caso de los *cyborgs*. Debemos tener en cuenta que, hasta el momento, no hay un significativo desarrollo, aunque ya hay casos, como el del artista Neil Harbisson, que había sufrido una disfunción congénita que le impedía distinguir más tonalidades que el blanco y el negro, se lo trató y en la actualidad se ha convertido en el *primer ser humano reconocido por un estado* y en la foto de su pasaporte de Reino Unido consta el *dispositivo que se ha implantado en la cabeza para ver los colores* y escucharlos con su dispositivo.

El tema a debatir, es en el marco de las modificaciones:

¿Qué naturaleza jurídica tiene el *cyborg*? ¿Humano o robot?

¿Cuáles son los límites jurídicos? Según el investigador de Robolaw, Andrea Bertolini, habrá que tener en cuenta la autodeterminación, la dignidad humana y la igualdad, principios que podrían ayudar a dirimir qué comportamientos están permitidos en cada circunstancia cuando se trate de dispositivos que llevan a los humanos más allá de sus capacidades.

El citado investigador sostiene que "la modificación de uno mismo no debería estar permitida porque la dignidad humana tiene que ser entendida como un límite objetivo a nuestra libertad", aunque considera que habría que estudiar el problema caso por caso y, por supuesto, en el caso de modificaciones, habría que abrir un marco a la discusión sobre personas con alto poder adquisitivo que podrían mejorarse tecnológicamente y quizás podrán conformarse ciudadanos de primera o se segunda según accedan o no a la tecnología de los *cyborgs*.

Por ahora deberemos recurrir a los principios generales del derecho que nos suministran herramientas aproximativas.

V. Carta sobre robótica

En el medio de todo este debate sustentado en arenas movedizas, se ha propuesto un código de conducta ética en el campo de la robótica que establecería las bases dirigidas a la identificación, la supervisión y el cumplimiento de los principios éticos fundamentales desde la fase de diseño y desarrollo.

En esa línea de pensamiento, se ha elaborado un Código de Conducta para los ingenieros en Robótica, en cuyo preámbulo se invita a los investigadores y diseñadores a actuar de forma responsable y con la máxima consideración dirigido a la necesidad de respetar la dignidad, intimidad y la seguridad de las personas.

Por otra parte, y en ese mismo documento, se invita a respetar los siguientes principios:

a) Beneficencia: los robots deben actuar en beneficio del hombre;

b) Principio de no perjuicio o maleficencia: la doctrina de «primero, no hacer daño», en virtud del cual los robots no deberían perjudicar a las personas;

c) Autonomía: la capacidad de tomar una decisión con conocimiento de causa e independiente sobre los términos de interacción con los robots;

d) Justicia: la distribución justa de los beneficios asociados a la robótica y la asequibilidad de los robots utilizados en el ámbito de la asistencia sanitaria a domicilio y de los cuidados sanitarios en particular.

Todo ello en el contexto de respetar los derechos fundamentales dirigidos a que las actividades de investigación en materia de robótica deben respetar los derechos fundamentales; y, por su parte, las actividades de concepción, ejecución, difusión y explotación, han de estar

al servicio del bienestar y la autodeterminación de las personas y de la sociedad en general.

La dignidad y la autonomía humana siempre deben respetarse, manteniendo asimismo que las actividades de investigación en el ámbito de la robótica deben llevarse a cabo de conformidad con el principio de precaución, anticipándose a los posibles impactos de sus resultados sobre la seguridad y adoptando las precauciones debidas, en función del nivel de protección, al tiempo que se fomenta el progreso en beneficio de la sociedad y del medio ambiente respetando asimismo la privacidad, salvo con consentimiento, siempre y en todo caso teniendo en cuenta el hecho de maximizar beneficios y reducir al mínimo los daños.

Buenas prácticas que esperemos se cumplan.

Se trata de una carta de buenas intenciones, aunque recordemos que de buenas intenciones está pavimentado el camino al infierno.

VI. Conclusiones

A esta altura de este trabajo, se presentan más dudas que certezas. ¿Deberá el fabricante asumir la responsabilidad en todos los casos? ¿Tendrán los robots «personalidad electrónica» cuando sean autónomos? ¿Cómo protegeremos nuestra privacidad cuando un robot doméstico conviva con nosotros?

Lo cierto es que ya se está analizando el marco normativo que podría aplicarse en un futuro a todo el panorama de la inteligencia artificial (17).

Pero, además, lo que se advierte es que este mundo nuevo no responde al esquema anterior, en el lenguaje, el derecho y en casi todos los órdenes (18).

Ahora vemos que no podemos esquivar los nuevos paradigmas sin hallar dificultades a cada paso.

Vemos que el progreso tecnocientífico está transformando los conceptos claves del derecho con los que hemos venido avanzando durante varias décadas y en verdad estamos perplejos.

El mundo del derecho siempre ha sido un refugio confortable para eludir nuevas ideas y conceptos. Sin dudas representa un gran esfuerzo poner en marcha esquemas novedosos y dinámicos que nos habiliten a encarar el cambio como si fuera un teléfono celular.

Los juristas debemos hacernos cargo de esos procesos y proponer el marco del derecho que, como siempre, es el gran ordenador de la sociedad.

Y también de los robots (19).

(17) Parlamento Europeo, 2014-2019, Informe con recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica, (2015/2103(INL)).

(18) Ver diversos informes sobre este apasionante tema:
Imagining a non-biological machine as a legal person
David J. Calverley, Bridging the Accountability Gap:Rights for New Entities in the Information Society?
Bert-Jaap Koops
Tilburg Institute for Law, Technology and Society (TILT)
e.j.koops@uvt.nl & Mireille Hildebrandt
Erasmus University Rotterdam (EUR) - Erasmus School of Law;
Vrije Universiteit Brussel
*hildebrandt@frg.eur.n*l & David-Olivier Jaquet-Chiffelle
Bern University of applied Sciences; University of Lausanne
David-olivier.jaquet-chiffelle@unil.ch
Tilburg University Legal Studies Working Paper Series No. 017/2010
July 23, 2010

(19) EUROPEAN CIVIL LAW RULES IN ROBOTICS, http://www.europarl.europa.eu/committees/fr/supporting-analyses-search.html

La inteligencia artificial en el Derecho

RUBÉN ASOREY (*)

Estamos ya ante la aplicación de la inteligencia artificial al derecho que, por un lado, parece una necesidad ineludible frente al fenómeno del *Big Data* y, por el otro, origina el interrogante de si será posible eliminar la subjetividad en su aplicación a la disciplina.

Se trata de indagar si será factible en el ámbito del derecho aplicar los referidos sistemas, aprovechando los beneficios del *Big Data*, término que en español se denomina "Datos Masivos", pero que no se utiliza sino en inglés para referirse al proceso de recolección de datos en grandes cantidades producto de la era digital, la expansión de Internet y el almacenamiento en la nube, cuyo análisis se efectúa por medios no tradicionales.

Este fenómeno produce sus repercusiones en el ámbito del derecho por la multiplicidad y diversidad de antecedentes que se pueden recoger de cada tema y la necesidad de contar con la rapidez de los buscadores que permiten tener la información necesaria para el análisis de cada problema legal.

Sin duda que, frente al fenómeno del *Big Data* en la vida jurídica, la aplicación de la inteligencia artificial está motivada a mitigar las situaciones que se producen en las distintas disciplinas jurídicas ante el agobio de la multiplicidad de datos para resolver problemas concretos.

Dada la necesidad de contar con la información que suministran las plataformas, surge el interrogante sobre la eliminación de la subjetividad para suministrar una resolución del caso en la aplicación de la inteligencia artificial al derecho, más allá que dichos sistemas permitan analizar en segundos toda la normativa, jurisprudencia y doctrina escrita sobre un tema.

El esfuerzo puesto en la aplicación de la inteligencia artificial al derecho debe tener como objetivo facilitar el trabajo del sujeto aplicador del derecho o de quien asesora sobre la problemática que origina, pero no puede pretender reemplazar la subjetividad humana por máquinas y *software* provistos de antecedentes del caso con la finalidad de obtener una respuesta.

El primer interrogante que surge es si será factible aplicar la inteligencia artificial en los procesos judiciales, tanto por parte del juzgador como de los abogados litigantes, prescindiendo de la subjetividad.

La respuesta negativa a ambos interrogantes está fundada en que no es posible encontrar so-

(*) Miembro honorario del Instituto Peruano de Derecho Tributario, del Instituto Ecuatoriano de Derecho Tributario, del Instituto Uruguayo de Estudios Tributarios, de la Asociación Venezolana de Derecho Tributario, de la Asociación Argentina de Estudios Fiscales. Miembro permanente del Directorio del Instituto Latinoamericano de Derecho Tributario; y expresidente de dicha entidad.

luciones a los conflictos que el derecho presenta sin el discernimiento humano de la cuestión.

Adicionalmente, en la resolución del conflicto, a las limitaciones que presenta la inteligencia artificial, más allá de sus beneficios, debe recordarse que "recolectar más datos no garantiza que sean precisos, ni que sean relevantes para cumplir nuestros objetivos, ni muchos menos capaces de poner esos datos al servicios de la justicia" (1).

También se destaca que el *Big Data* puede solidificar el *statu quo*, pues mientras la memoria biológica es un sistema fantástico de filtración y organización de la información, que recuerda lo importante, olvida lo insignificante, reconstruye el pasado constantemente y le da distintos valores a diferentes memorias, las memorias digitales lo recuerdan todo sin reinterpretarlo, ni valorarlo, es la antítesis de la memoria biológica (2).

Por ello, toda sentencia podrá recurrir a los beneficios de la inteligencia artificial, usufructuando las plataformas que facilitan la convivencia con el *Big Data*, pero siempre la decisión pasará por la subjetividad del sentenciante.

Similar conclusión deviene en el conocimiento y resolución de los problemas profesionales.

En efecto, en la ejecución de las tareas profesionales de asesoramiento, cualquiera sea la forma que se materialice, como señalaba ya en la década del ochenta del siglo pasado el profesor Alvin Warren (3) de la Universidad de Harvard en relación con cierta parcela del derecho, los asesores, en cumplimiento de sus tareas profesionales, deben arribar al recto juicio frente a la consulta de sus clientes para poder determinar si las transacciones son o no legalmente posibles, con la particularidad que frecuentemente el cliente llega con un esquema de propia elaboración.

Frente a tal tipo de situaciones, muchas veces el letrado asume el riesgo de encontrarse en la incómoda posibilidad de aparecer como una mente negativa o un enfoque conservador que perjudica los intereses del cliente.

En algunas materias, este riesgo ha sido atenuado con la sanción de las leyes penales y su posterior aplicación por los tribunales a la parcela del derecho en consulta, que permite al cliente tomar conciencia de las diferencias entre las transacciones seguras con beneficios, las riesgosas y las claramente ilegales y evaluar las consecuencias de su decisión a la luz de las consecuencias para su persona y su familia.

Además de las eventuales consecuencias penales, otro factor que también influye sobre la necesidad de tomar el asesoramiento con mayor optimización pero evitar conductas ilegales se origina en la gravosa carga de tener que asumir con retroactividad la consecuencia de la conducta inapropiada o ilegítima.

Debe evitarse en la vida profesional una de las falacias que se le atribuye al optimismo del *Big Data*, el cual es creer que cuantos más datos tengamos mejor resolvemos los problemas. Para ello, debemos recordar al poeta T. S. Elliot "¿Dónde está la sabiduría que hemos perdido con el conocimiento? ¿Dónde está el conocimiento que hemos perdido con la información?" (4).

Para evitar tal riesgo, el asesor debe, en primer término, profundizar los hechos manifestados por el cliente, que suele desconocer cuál es la información importante o no para resolver la consulta.

Tales hechos, como señalaba Warren, "deben ser puestos en orden, estudiados y escudriñados; no debe haber piezas sueltas. Una vez que están definitivamente alineados y revestidos con las inferencias y conclusiones que le son propias, el asesor debe tomar distancia de ellos y verlos como si fueran a desfilar ante una Corte, observándolos con gran sensibilidad y espíritu crítico" (5).

(1) Véliz, Carissa, Uehiro, Centre for Practical Ethics, Wellcome Centre for Ethics and Humanities, Universidad de Oxford, El País, 14 de junio de 2019.

(2) Véliz, Carissa, cit.

(3) Revista del IDTP N° 7, diciembre, 1984.

(4) ELLIOT, T. S., *El Primer Coro de la Roca*, 1934.

(5) Revista del IDTP N° 7, diciembre, 1984.

Otro de los aspectos trascendentes es evaluar cómo pueden ser probados tales hechos ante los tribunales. Este es un aspecto esencial, el más importante, para obtener una resolución favorable ante el eventual conflicto que pueda tener el cliente en el futuro, pues las causas no se ganan solo por los argumentos de derecho sino por la prueba de los hechos.

Debe evaluarse cuándo la aplicación de los antecedentes con la que se cuenta convierte al asesoramiento en adecuado. Nos referimos a que, en el consejo, debe evitarse el riesgo que sea limitado y técnico. Como señaló Josh Billings, el problema con los especialistas "no es lo que no saben, sino lo mucho que saben que no es cierto" (6).

Se debe agregar a la más alta competencia técnica la bondad de juicio, que es la característica de todo asesor experimentado. No debe dejarse traicionar por su propia pericia técnica; antes bien, debe entender que ella es solo un medio para formular juicios informados, pero no puede por sí misma sustituir al discernimiento. El asesor debe bregar para elevarse por encima de la mera competencia técnica y para desarrollar una amplia perspectiva y una sindéresis, que no serán obstruidas por la sensación de un conocimiento y experiencia superiores en su área ni por la impresión de que todas las reglas y principios están tornándose un caos (7).

Los algoritmos nos ayudarán, a través de los sistemas y los *softwares*, a afrontar el desafío del *Big Data*, pero nunca podrán sustituir al magistrado ni al letrado en la interpretación y en la aplicación del derecho.

(6) Revista del IDTP N° 7, diciembre, 1984.

(7) Revista del IDTP N° 7, diciembre, 1984.

Un paso atrás en la protección de los datos biométricos del sospechoso

CHRISTIAN H. MILLER (*)

I. Introducción

En los últimos meses, la jurisprudencia de los Estados Unidos avanzó notablemente en el entendimiento de que el desbloqueo forzoso de un dispositivo electrónico mediante datos biométricos del sospechoso debería ser asimilado como testimonial y, por ende, autoincriminatorio en el sentido de la Quinta Enmienda (1).

El razonamiento de dicha línea radica en tildar de "irrazonable" (2) a toda búsqueda o incautación que atropelle derechos esenciales de una persona, como el de no autoincriminación. Y, según esta doctrina, obligar a alguien a desbloquear su teléfono mediante el uso de sus huellas digitales podría conducirlo a ser testigo contra sí mismo, lo que está prohibido por la Constitución de dicho país.

Sin embargo, recientemente, el juez de la Corte del Distrito de Idaho, David Nye, concedió una moción presentada por la fiscalía y revirtió (3) la sentencia del juez magistrado Ronald Bush que negaba una orden de allanamiento adicional para acceder (apoyando los dedos del detenido) al contenido del Google Pixel 3XL secuestrado, poniéndole un freno a la novedosa teoría.

Es que, en el caso, el juez Nye entendió (4) que "aplicar la huella digital en el sensor es simplemente tomar una característica física (que) por sí sola no comunica nada", y por ello concluyó que "la orden solicitada, no violaría la Quinta Enmienda (ya que no implicaría por sí misma) ninguna prueba testimonial". Lo que nos deja servido el debate.

II. El caso

En el marco de la investigación de un caso de tenencia de pornografía infantil, la fiscalía consiguió una orden de registro sobre el sospe-

(*) Abogado (UCA). Especialista en Derecho de alta tecnología (UCA) con formación en Cibercrimen y evidencia digital (UBA) y en Protección de datos personales, privacidad y compliance (UP).

(1) Traducido del inglés, "Nadie estará obligado a responder por un delito castigado con la pena capital o con otra infamante si un jurado no lo denuncia o acusa (…) ni se le forzará a declarar contra sí misma en ningún juicio criminal; ni se le privará de la vida, la libertad o la propiedad sin el debido proceso legal; ni se ocupará su propiedad privada para uso público sin una justa indemnización".

(2) "Una búsqueda e incautación es irrazonable y, por lo tanto, ilegal, si viola los derechos de la Quinta Enmienda de la persona" (traducido del inglés), de *Boyd v. United States*, 116 US 616, 630, 1886.

(3) Según facultades previstas en 28 USC § 636(b)(1)(A): "Un juez de la corte puede reconsiderar cualquier asunto previo al juicio bajo este subpárrafo (A) donde se demuestre que la orden del juez magistrado es claramente errónea o contraria a la ley" (traducido del inglés).

(4) Caso N° 1:19-mj-10441-DCN, 26/07/2019.

choso, un vehículo y su residencia, que autorizó además la incautación de cualquier computadora de escritorio o portátil, teléfono móvil, tableta, servidor y/o cualquier otro *hardware* de red que pudiera constituir "evidencia de la comisión" del delito penal.

Fue así que, en el baño de la vivienda, la policía halló un teléfono Google Píxel 3XL "bloqueado" con datos biométricos del sospechoso y para el cual solicitó una orden de registro adicional, con intenciones de obligarlo a desbloquear el artefacto incluso presionando sus dedos contra el sensor o lector de huellas dactilares.

Sin embargo, el Tribunal a cargo del mencionado juez Ronald Bush denegó (5) la orden amparándose en la Cuarta Enmienda (6) por "irrazonable", asimilando al uso forzoso de la huella dactilar con la autoincriminación. Es que, según el criterio adoptado, al desbloquear el teléfono, el sospechoso reconocería la propiedad y el control exclusivo sobre el dispositivo, así como la autenticidad de los contenidos incriminatorios allí almacenados.

Para el juez, las garantías previstas contra la autoincriminación "no se limitan a las comunicaciones verbales o escritas", sino que los actos que impliquen afirmaciones de hecho deben ser considerados como tales también. Y se justificó diciendo que el sentido de la Cuarta Enmienda radica justamente en colocar a un magistrado entre el ciudadano y las fuerzas policiales (7), pero no para proteger a los criminales sino para que un tercero objetivo pueda sopesar la necesidad de invadir la privacidad del sospechoso y de los terceros expuestos, lo que a su juicio aquí es palmariamente irrazonable.

Luego, ante la negativa del juez Bush, la fiscalía presentó una moción con la cual logró que se revirtiera el fallo.

III. Las posturas

El derecho a guardar silencio se ha consagrado como un acto de defensa e incluso como un medio para acabar con los tormentos cuyo fin era la confesión del acusado (8). De hecho, su consecuente garantía de no autoincriminación compulsiva va más allá e incluye todas aquellas situaciones en las que el sospechoso pudiera convertirse en testigo contra sí mismo. Y, si bien es verdad que no se trata de un instituto propio del derecho moderno, resulta destacable su aparición en la Declaración de Derechos de Virginia (9) (natural antecedente de la Quinta Enmienda), donde ya se establecía que el acusado no puede ser obligado a suministrar pruebas que lo incriminen.

Empero, el creciente uso de dispositivos electrónicos pareciera poner en crisis este paradigma. Es que uno de los fenómenos más destacables de esta era es la digitalización de todos los planos de la vida humana, tanto pública como privada, cuyo epicentro son los teléfonos móviles y su capacidad de conectarnos al mundo mediante Internet. Hablamos de un "yo digital" que se corresponde con alguien "real" (a un ritmo asombroso (10)) mediante documentos, costumbres, relaciones y hasta pensamientos registrados y almacenados en pequeños aparatos que llevamos con nosotros

(5) Sentencia del 8/05/2019.

(6) Traducido del inglés, "El derecho del pueblo a la seguridad en sus personas, casas, documentos y efectos contra perquisiciones y secuestros irrazonables no será violado, y no se expedirá ningún mandamiento sino en virtud de causa probable apoyada por juramento o afirmación y que describa con precisión el lugar que debe ser registrado y las personas o cosas que deben ser detenidas o secuestradas".

(7) Cita de Johnson v. United States, donde la Corte de ese país señaló: "En qué casos el derecho a la privacidad debe razonablemente ceder a favor del derecho estatal a practicar una requisa, es algo que, como regla, debe ser decidido por un Juez; no por un policía ni por ningún otro agente del Gobierno".

(8) En nuestro Código Procesal Penal, el art. 296 establece que "En ningún caso se le requerirá juramento o promesa de decir verdad ni se ejercerá contra él coacción o amenaza ni medio alguno para obligarlo, inducirlo o determinarlo a declarar contra su voluntad ni se le harán cargos o reconvenciones tendientes a obtener su confesión".

(9) Adoptada el 12/06/1776, en su art. 8° establece que "en todo juicio capital o criminal (...) tampoco se le puede obligar a presentar pruebas contra sí mismo..." (traducido del inglés).

(10) En 2014, ya se enviaban por minuto 204 millones de correos electrónicos, se "subían" 72 horas de video a YouTube y se realizaban más de 2 millones de búsquedas por Google.

a cada lugar a donde vamos. Se trata de un registro completo de nuestra intimidad (por fuera de nuestra mente, portable y concentrado en un solo sitio) que afecta a toda expectativa de privacidad —propia y de terceros—, y más aún desde la popularización de la biometría como herramienta de seguridad.

Porque al principio solo teníamos que "deslizar para desbloquear", pero luego llegaron las contraseñas numéricas, las alfanuméricas y los patrones de puntos y más tarde el cifrado de cierta información sensible. De hecho, en los nuevos modelos, los fabricantes de teléfonos móviles incorporaron ya poderosos sensores de datos biométricos capaces de reconocer la huella digital, el rostro y hasta el iris. Y con ello dieron inicio a un debate del cual probablemente no tengan noticias.

Es que, para el derecho penal, existen pruebas que toman al ser humano como "objeto" y como "sujeto" (11), donde la mente es el límite jurídico para la autoincriminación (12). Y la jurisprudencia estadounidense, en general, había logrado cierta estabilidad al entender que el acusado no puede ser obligado a proporcionar el código de acceso a su teléfono móvil porque "es testimonial y está protegido por la Quinta Enmienda" (13). Sin embargo, con la aparición de los lectores biométricos, que no necesitan de una expresión verbal o escrita para desbloquear el dispositivo sino que reconocen automáticamente los rasgos conductuales o físicos del que tiene el control del mismo, esta supuesta unidad de criterio fue puesta en duda.

Para el juez Bush, cuyo principal sustento es el fallo de la jueza de distrito Kandis Westmore (California) (14), la evidencia podría calificarse como testimonial si confirma la posesión y el control sobre el dispositivo y consecuentemente la autenticidad de los documentos incriminatorios allí almacenados. En cambio, para el juez Nye, aquí no hay expresión alguna. Sino que entiende necesaria la diferenciación entre obligar a comunicar algo y obligar a proporcionar una característica física, porque para él "la huella digital por sí sola no comunica nada… ni requiere que el testigo divulgue nada a través de sus procesos mentales".

IV. El antecedente

El precedente inmediato de fallo del juez Bush es, sin lugar a dudas, la decisión de la jueza Westmore. Es que, en el marco de la investigación de un caso de "sextorsión", la fiscalía solicitó autorización para registrar el domicilio de quienes habrían coaccionado a la víctima mediante Facebook Messenger con la divulgación de un video íntimo y, si bien la jueza admitió que existían indicios suficientes como para respaldar una "causa probable" en cuanto al registro, denegó la solicitud por devenir violatoria de las garantías previstas en las Enmiendas Cuarta y Quinta.

El pedido incluía la capacidad de secuestrar todo elemento que pudiera estar relacionado con la realización del delito, así como la potestad de obligar "a cualquier persona presente al momento del registro a presionar un dedo (incluido el pulgar) o utilizar otras características biométricas, como reconocimiento facial o de iris, con el propósito de desbloquear los dispositivos digitales encontrados con el objeto de permitir una búsqueda de los contenidos según lo autorizado por la orden de registro" (15).

Pero Westmore entendió que, aún en el proceso de ejecución de una orden de registro

(11) De Luca, Javier, "El Cuerpo y la Prueba", *Revista de Dcho. Procesal Penal*, Rubinzal Culzoni, 2007, N° III, p. 41.

(12) "Por la propia naturaleza de la cosa, por resultar productos de la mente humana, quedarán excluidos de esta categoría los cuerpos de escritura, las reconstrucciones de hechos, las requisitorias de aportes de datos o documentos, las declaraciones de toda índole y varias más que provengan del mismo origen. En cambio, las fotografías, los registros de las huellas dactilares, la requisa de sus pertenencias, la sujeción mediante esposas, su conducción a la sala de audiencias, las ruedas de reconocimientos de personas, arrancarle un pelo, la extracción de sangre, la toma una radiografía, la recolección de saliva, etcétera, no participan de aquel origen y en tales prácticas el sujeto es considerado como objeto de prueba"; Fiscalía General N° 4 ante la Cámara Federal de Casación Penal, Dictamen N° 9.240: "Cuba, Lidia Paola s/ Recurso de casación", Causa Nº CPE 573/2013/TO1/CFC1, 6/10/2014.

(13) Commonwealth v. Baust, 89 Va. Cir. 267, 271 (Va. Cir. Ct. 2014), traducido del inglés.

(14) Caso N° 4:19-mj-70053-KAW.

(15) Traducido del inglés.

válida, la vulneración desproporcionada de cualquier otro derecho fundamental (como la privacidad) intrínsecamente tacha a toda búsqueda e incautación de irrazonables. Y, según su parecer, la amplitud excesiva de la solicitud planteada (contra "cualquier persona", incluso contra quien no fuera indicado como sospechoso, y/o dispositivos encontrados) es lo que primeramente atenta contra su legalidad. En definitiva, determinó la falta de motivación para forzar a todos los presentes a utilizar sus datos biométricos en los artefactos hallados.

Y eso no es todo, porque la jueza de California advierte que incluso si existiera una causa probable suficiente no se podría otorgar la medida solicitada. Es que, obligar al sospechoso a desbloquear el dispositivo electrónico mediante el uso de sus datos biométricos sería conducirlo a "ser testigo contra sí mismo", lo que está prohibido por la Quinta Enmienda. De esta manera, asimiló a dicho desbloqueo con el concepto de declaración que la ley prevé como autoincriminatorio.

Así, la jueza reubicó jurídicamente (y dotó de mayores garantías) a las últimas novedades en desbloqueo de dispositivos electrónicos (16). Comprendió que la protección que la Quinta Enmienda les otorga a las contraseñas numéricas y alfanuméricas debe lógicamente extenderse al método de desbloqueo biométrico, cuyo sentido es idéntico al de las primeras. Es tajante al sostener que la prohibición del testimonio autoincriminatorio no puede limitarse solo a la comunicación verbal o escrita, sino que "los actos que impliquen afirmaciones de hecho" deben considerarse como tales también. Y más aún teniendo en cuenta que, mediante un acto propio como es el sistema de desbloqueo biométrico, se reconoce tanto la posesión, el acceso previo y el control sobre el dispositivo, así como la autenticidad de los documentos digitales almacenados (e incluso desconocidos para la investigación) y que podrían incriminarlo irrefutablemente.

Westmore es muy clara contrastando al desbloqueo obligatorio mediante datos biométricos con los medios compulsivos de prueba como la extracción de muestras de sangre, saliva, huellas dactilares, etc., que utilizan "el cuerpo" del sospechoso como herramienta pero que no logran obtener una "expresión del contenido de la mente" del individuo. Destaca que la ley admite determinadas injerencias con prescindencia de la voluntad y consentimiento del sospechoso, pero que el límite siempre será su conciencia.

Porque, a su criterio, con un simple toque en la pantalla del teléfono (e incluso sin tocarla), el sospechoso podría confirmar todo lo que se almacene detrás de ese bloqueo digital y con ello nos encontraríamos frente a una medida de prueba que claramente excede los fines de constatación que son propios de los medios de evidencia "física".

La magistrada sostiene que el objetivo de someter al sospechoso —por ejemplo, a la extracción de huellas digitales— es simplemente cotejar sus registros con la evidencia física encontrada previamente en la escena del crimen, lo que a todas luces se desmarca del mundo inimaginable, desconocido y desproporcionado que podría hallar la fiscalía al inmiscuirse dentro de la información más privada de alguien (y de los terceros con los que interactuó), la cual no puede ser refutada en forma alguna justamente por la exclusividad de los datos biométricos utilizados al configurar el bloqueo del dispositivo.

Lo que para el juez Bush es análogo a entregar la llave de una caja fuerte (17), para la jueza de California es un avasallamiento irrazonable sobre la privacidad del sospechoso y de terceros, e incluso violatorio de la Quinta Enmienda en cuanto implicaría el reconocimiento de toda documentación autoincriminatoria contra la cual es imposible defenderse.

V. Conclusión

Ante la aparición de nuevas tecnologías, el derecho se encuentra en ocasiones ante la ne-

(16) En Carpenter v. United States (138 S. Ct. 2206, 2213, 201 L. Ed. 2d 507, 2018), la Corte Suprema de los Estados Unidos instó a sus tribunales a salvaguardar los derechos constitucionales por sobre el avance de las tecnologías adoptando reglas que tengan en cuenta a los sistemas más sofisticados.

(17) Citando la comparación realizada por la Corte Suprema en Doe v. United States, 487 U.S. 201, 219, 1988.

cesidad de resolver situaciones no previstas —ni remotamente— por la ley, forzando su contenido y emparentando erróneamente lo analógico con lo digital. Y para el derecho penal, el punto más álgido pareciera encontrarse en la recolección de evidencia digital, momento crítico en el cual interactúan operadores de la justicia, derechos, garantías y nuevas tecnologías.

Al respecto, Marcos Salt nos advierte que "todo el sistema de prueba fue diseñado teniendo en cuenta la evidencia física y no la evidencia digital (…) esta pretensión de aplicar ´por analogía´ (…) además de ser cuestionable desde un punto de vista constitucional, genera inconvenientes tanto en términos de ´eficiencia´ estatal en la investigación de los delitos como en lo que respecta a una adecuada protección de las garantías tanto del imputado como de terceros que pueden ser afectados (…) en el marco de una investigación penal", y concluye que "la investigación de cualquier delito (incluso los más tradicionales como un robo o un homicidio) en la que sea necesaria la obtención de evidencia digital, demanda cambios de funcionamiento en los organismos de persecución penal" (18).

En la misma línea, la organización no gubernamental Asociación por los Derechos Civiles (ADC) sostiene que "la dificultad desde el punto de vista jurídico se ha agravado pues el avance de las tecnologías y la utilización de Internet en la vida cotidiana, ha llevado la cuestión informática a cualquier investigación de cualquier tipo de hecho. La evidencia digital -junto sus complicaciones- hoy atraviesa el sistema de manera transversal (cualquier caso menor y simple hasta los más complejos y casos de derecho penal común, como de cuello blanco). Ello es lo que plantea los mayores desafíos desde el examen del derecho procesal penal y la vigencia de las garantías…" (19).

Resulta evidente que la popularización de ciertas tecnologías es capaz de alterar diversos ámbitos de la vida humana, pero la aparición del *smartphone* (cuya mayor virtud es conectarse a Internet) lo cambió todo. Es que, en apenas una década, pasó de ser un distintivo de las clases más acaudaladas a estar en manos de casi toda la población (20). Somos partícipes de una era híper social —cuya tecnología es tremendamente simple, accesible y transportable— que ha superado la simple cuestión filosófica demostrando capacidad real de dañar al propio ser, a su intimidad e incluso al desarrollo de su personalidad.

Sin notarlo, hombres y mujeres pasaron del exclusivo consumo de información a registrar toda su vida privada en pequeños teléfonos móviles, por lo cual deviene necesario reconocer la extrema digitalización que avanza prácticamente sobre todos los planos: imágenes, costumbres, relaciones, sentimientos y hasta pensamientos. Todo un "yo digital" que cada día se parece un poco más al "yo físico".

De esta manera, contemplar la posibilidad que con un simple toque sobre la pantalla (e incluso con solo mirarla), el sospechoso de un delito podría estar dando acceso a toda esa información, parece un tanto desproporcionado. No solo por significar un avasallamiento sobre su intimidad y la de terceros, sino porque también implicaría someterlo a entregar evidencia potencialmente incriminadora.

Necesariamente el Estado, en el ejercicio de su poder punitivo, debe restringir en ocasiones ciertos derechos, pero ¿hasta dónde puede ser afectada la dignidad humana? ¿Hasta dónde puede separada la persona del principio de inocencia? Los fallos comentados aquí se colocan deliberadamente en veredas opuestas apenas preguntándose qué hacer con los sensores biométricos que traen los teléfonos móviles más populares de hoy en día. Y si bien coinciden en que las autoridades no pueden obligar al sospechoso a aportar las claves de acceso a su dispositivo (lo que sería testimonial en el sentido de

(18) Salt, Marcos, *Nuevos desafíos de la evidencia digital: Acceso transfronterizo y técnicas de acceso remoto a datos informáticos*, Ad-Hoc, 2017, p. 18.

(19) Sergi, Natalia, "Análisis jurídico de la situación de la evidencia digital en el proceso penal en Argentina", Asociación por los Derechos Civiles, 2018, p. 2.

(20) Según la Encuesta Nacional sobre Acceso y Uso de Tecnologías de la Informática y la Comunicación —INDEC, 2013—, en nuestro país, el 40% de los hogares tiene como mínimo una computadora con acceso a Internet —en la Ciudad de Buenos Aires, el 75%— y más del 85% por lo menos un teléfono celular).

la Quinta Enmienda), discrepan en cuanto a la capacidad de someterlo a utilizar sus datos biométricos en los sensores del mismo.

Sin embargo, la digitalización de la intimidad va en aumento y no resulta lógico disminuir su protección ante la aparición de nuevas tecnologías. Es que los lectores biométricos vinieron a mejorar las medidas de seguridad del dispositivo personal incrementando toda expectativa de privacidad de los usuarios (al superar a las viejas claves de cuatro y seis dígitos numéricos), y no al contrario.

Parece excesivo dotar de poder de coacción a la policía frente a la existencia de lectores de huellas digitales, rostro e iris, cuando el resultado que se obtendrá es el mismo que al obligarlo a proporcionar su clave de acceso y el sospechoso se verá de igual manera sometido a reconocer tácitamente todo contenido incriminatorio —y tal vez desconocido por la investigación—. Hoy por hoy, el teléfono móvil es un inventario completo de nuestra intimidad y por ello las medidas de seguridad aumentan cada año, como así también debe hacerlo la justicia.

En definitiva, se deduce esperable que toda tutela que el derecho haya depositado sobre los más antiguos métodos de bloqueo electrónico sea extrapolada a los más novedosos. El contenido digital que se oculta bajo contraseña numérica no será diferente al que se esconde bajo reconocimiento dactilar o facial. Lleva consigo (cuando menos) las mismas expectativas de privacidad, por lo cual deviene absurdo el razonamiento que le quita protección constitucional al método que utiliza sensores biométricos.

A su vez, el derecho penal se ha preguntado si forzar a un sospechoso a desbloquear un dispositivo mediante sus datos biométricos es asimilable a otros tipos de prueba compulsivos (que incluso podrían resultar autoincriminatorios) como la extracción de sangre, saliva, huellas, etc., y la respuesta debe ser tajante: NO.

Como bien sostiene la jueza Westmore, mientras la toma de impresiones digitales tiene por objeto el contraste con alguna muestra obtenida de la escena del crimen —y da lugar a la defensa—, el ingreso forzoso mediante la huella digital del sospechoso al artefacto podría implicar la colaboración expresa (y obligatoria) cuya consecuencia directa sería la autenticación de los contenidos digitales allí almacenados (e incluso de los desconocidos por la investigación), lo cual se acerca en demasía al testimonio contra uno mismo que prohíbe la ley.

Por lo expuesto, se comparte el criterio del juez magistrado de Idaho, Ronald Bush, en el entendimiento de que el desbloqueo forzoso del dispositivo electrónico mediante datos biométricos del sospechoso debiera ser asimilado como testimonial y, por ende, autoincriminatorio en el sentido de la Quinta Enmienda.

La ciberseguridad como política de Estado. Estrategia Nacional de Ciberseguridad. Decreto 829/2019. Protección de los datos e intimidad personal

HUGO ALFREDO VANINETTI (*)

I. Introducción

La ciberseguridad y la ciberdefensa deben ser consideradas como áreas estratégicas para todo Estado.

La vertiginosa expansión de internet, de la Internet de las Cosas (IoT) (1) y hasta de las ciudades inteligentes (*smart cities*) (2) está ocasionando una alta interconectividad de sistemas cada vez más complejos mediante la gestión de datos a gran escala (*Big Data*) y la inteligencia artificial.

Si bien este nuevo contexto ha traído numerosos beneficios en los más diversos ámbitos, origina, a su vez y por contrapartida, que crezcan exponencialmente las amenazas y ataques cibernéticos a los mencionados sistemas aprovechándose de las vulnerabilidades existentes mediante diferentes actividades maliciosas o debido a errores humanos involuntarios.

Los aludidos ataques cibernéticos pueden ocasionar altos y eficaces resultados con escasa infraestructura en cuanto a recursos humanos y materiales para concretarlos radicando allí su

(*) Abogado. Consultor informático. Autor de los libros *Aspectos jurídicos de Internet* y *Responsabilidad jurídica de los buscadores*, ambos de Librería Editora Platense.

(1) A la Internet de las cosas (en inglés, *Internet of Things*, abreviado IoT) se la puede definir como todo sistema interconectado de objetos físicos que utilizan sensores con capacidad para interrelacionarse entre sí y/o con las personas e intercambiar datos por internet. La Internet de las Cosas implica la interconexión e interrelación de objetos cotidianos con internet. El término fue acuñado en 1999 por Kevin Ashton, un investigador del Instituto de Tecnología de Massachusetts (MIT por las iniciales de su nombre en inglés, Massachusetts Institute of Technology).

(2) El concepto de *Smart City* (ciudad inteligente) se estructura en el marco de la eficiencia energética y la sostenibilidad, persiguiendo un equilibrio entre el medio ambiente y el consumo de los recursos con los que dispone (humanos y materiales) para lo cual la autoridad municipal se apea de las diferentes herramientas que puede brindar las tecnologías de la información y del conocimiento. Una ciudad inteligente contará, para ser considerada como tal, entre sus herramientas de gestión con una moderna página web oficial del municipio a los fines que interactúe con el vecino; portales para realizar trámites *on line*; *software* destinado para el manejo interno de todo lo concerniente a la gestión municipal; sistemas para el control ambiental de la ciudad, para optimizar el servicio de acopio y tratamiento de reciclaje de residuos domiciliarios; la gestión del alumbrado mediante la sincronización con las horas solares; para el área de seguridad (televigilancia), el control en cuanto a prestación y calidad de los servicios que brinde el municipio para optimizarlos (calidad del agua potable, por ejemplo). A su vez, las TIC´s pueden ser empleadas en una ciudad inteligente para establecer alertas tempranas ante eventuales fenómenos climáticos severos. Una ciudad inteligente busca, además, incrementar a través de las TIC´s la participación ciudadana en la toma de decisiones para brindar un mejor servicio público consultándolos vía redes sociales y distintas herramientas *on line*.

mayor peligrosidad y, porque además, los ataques pueden apoyarse en la ubicuidad y extraterritorialidad del medio para garantizar mayor impacto y cierto grado de impunidad.

Frente a este complejo cúmulo de amenazas viabilizadas en el ciberespacio (3), tanto endógenas como exógenas, como se verá más adelante, se erigen estrategias para enfrentarlas desde el sector privado, pero además por parte de cada Estado y organismos supranacionales, bajo la premisa de que se trata de proteger aéreas y cuestiones vitales que hacen a la seguridad nacional tanto para sus bienes, recursos y potencialidades estratégicas, como así también para los derechos de cada uno de sus ciudadanos a través del amparo de los datos personales.

II. Ataque cibernético

Se puede definir a un ataque cibernético como aquella acción iniciada desde una computadora, terminal o un sistema informático que compromete la confidencialidad, integridad o disponibilidad de la información almacenada en otra computadora, terminal o sistema informático.

Los ataques cibernéticos pueden tener distintas motivaciones, entre ellas, del tipo económico, social, propagandístico, militar o político y se llevan a cabo, muchas de ellas, a través de Internet.

Este tipo de ataques son dirigidos a las personas en forma particular o general, a organizaciones privadas o Estados y puede ser direccionado mediante *software* malignos (virus), tanto para afectar al *hardware* introduciendo órdenes incorrectas destinadas a destruir computadoras o sistemas informáticos afectando, por ejemplo, los sistemas de refrigeración, como para afectar al *software* mismo, que hace funcionar todo sistema informático.

Vale mencionar que existe una amplia y variada gama de ataques informáticos, algunos de los cuales pueden ir desde sobrecargar la demanda de información de un sitio específico, afectar áreas estratégicas de un Estado para que colapse, hasta introducir virus informáticos para desplegar acciones de espionaje, captura de información y datos personales, etc.

III. Efectos de los ataques cibernéticos

Se pueden clasificar los efectos de un ataque cibernético tanto en directos como indirectos.

Directos porque el ataque informático puede producir daños en redes o sistemas militares o proveedores del sector militar (4), y también en áreas sumamente estratégicas, sensibles y críticas por los servicios que brinda, como la salud, el sistema de finanzas, el tráfico aéreo, las comunicaciones, los servicios de electricidad, la provisión de agua potable, etc.; y también pueden generar daños *indirectos*, porque, en todos estos casos, el impacto que produce el daño en dichas redes y sistemas afecta a las personas poniéndolas en un peligro evidente e inminente.

Basta tan solo ejemplificar el daño que produciría a las personas un ataque informático en el tráfico aéreo, o si se alterara el suministro de energía, o bien en sus ingresos al afectarse un sistema financiero.

IV. Quiénes pueden originar ataques cibernéticos

Como bien lo advierte el documento denominado Estrategia Nacional de Ciberseguridad de España del año 2019, "debido a la revolución de Internet, Estados, grupos organizados, colecti-

(3) Para la Unión Internacional de las Comunicaciones, el ciberespacio es el "terreno físico y no físico creado por y/o compuesto de algunos o todos de los siguientes elementos: Ordenadores, Sistemas informáticos, Redes y programas informáticos, datos (Información, contenido y tráfico) y usuarios". Fuente: Baretto, Juan Fernando, "La guerra cibernética", *http://www.cefadigital.edu.ar/bitstream/123456789/1061/1/TFM%2004-2018%20BARETTO.pdf.*

"El Ciberespacio, nombre por el que se designa al dominio global y dinámico compuesto por las infraestructuras de tecnología de la información, incluida Internet, las redes y los sistemas de información y de telecomunicaciones", extraído de los considerandos de la Resolución 829/2019. Estrategia Nacional de Ciberseguridad de la República Argentina.

(4) En este sentido, se ha publicitado la información de que empresas tan sensibles como Lockheed Martin, el principal proveedor de tecnología del Pentágono en los EEUU, tuvo que reconocer en 2011 frecuentes 'ciberataques'. Fuente: "*Ciberamenazas: algo está cambiando*", *El Mundo*, España, 21 de febrero de 2013.

vos y hasta individuos aislados pueden alcanzar un nivel de poder y una capacidad de influir impensable en otros tiempos. La conectividad digital lleva a que los movimientos sociales globales tengan una importancia estratégica hasta hace poco subestimada".

Ante dicho contexto, los principales gestores de las amenazas en el ciberespacio pueden ser:

- Estados

Pueden realizar distintas acciones que van desde el espionaje, campañas de desinformación sobre cuestiones sensibles de otros Estados (5), ataques a infraestructuras sensibles (6) hasta medidas de defensa, ataque y exploratorias en un escenario de ciberguerra (7) que, como bien se ha señalado, "los ataques cibernéticos serán un componente significativo de cualquier conflicto futuro, ya sea que involucren naciones principales, estados paria o grupos terroristas" (8).

La potencialidad en el daño que pueden ocasionar estos ataques no se condice muchas veces con la cuantía de los recursos financieros ni humanos que se destinan a producir dichos daños, como ya fuese referenciado, puesto que el desarrollo de un virus puede demandar poca inversión de tiempo y recursos y producir daños incalculables en su oponente. Estaríamos frente a un supuesto de guerra asimétrica donde el objetivo central del más débil, para superar una fuerza militar más poderosa, será descubrir y explotar al máximo sus debilidades y brechas de seguridad en los sistemas informáticos estratégicos. En dicho contexto, un país poco desarrollado podrá inclusive contar con la opción de causar severos daños a un adversario poderoso en el marco de un hipotético campo de batallas digital.

- Hackers y hacktivistas

Pueden ser individuos aislados o grupos que se dedican a realizar prácticas de hackeo, ya sea con fines denominados éticos, buscando vulnerabilidades en los sistemas y así denunciarlos, o bien para generar daños.

El hacktivismo, por su parte, es un movimiento con fines propagandísticos y de protesta en torno a la defensa de ciertos temas (políticos, ecología, anti tecnología, etc.) a través de la

(5) "La denunciada injerencia de Rusia mediante un complejo plan de desinformación mediante fake news en el proceso electoral de los EEUU del año 2016". Consultar: "Rusia- Trump: la investigación de la injerencia del Kremlin en las elecciones de EE.UU. en 300 palabras", BBC Internacional, 22 de marzo de 2019, *https://www.bbc.com/mundo/noticias-internacional-46400948*.

(6) Según el New York Times, en diciembre de 2015, una unidad de inteligencia rusa cortó la electricidad a cientos de miles de personas en Ucrania occidental. Un equipo de expertos estadounidenses fue enviado para examinar los daños y concluyó que una de las mismas unidades de inteligencia rusas que causó estragos en Ucrania había hecho avances significativos en la red energética de Estados Unidos, como así también intentos de intrusión en centrales atómicas (Kansas y Nebraska) donde se afectaron sus comunicaciones pero no su control. En dicho contexto, el periódico denuncia que los EEUU ha llevado a cabo acciones de contraofensiva cibernética afectando la provisión de energía en ciertas regiones de Rusia. Fuente: "U.S. Escalates Online Attacks on Russia's Power Grid", *New York Times*, June 15, 2019. *https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html*.

(7) Se ha tomado conocimiento de ataques de este tipo. En 1993, Rusia no solo intervino militarmente con armas tradicionales sobre Georgia, sino que estuvo acompañada por un ciber ataque que la dejó aislada del resto de Europa y los Estados Unidos.

Tal vez el más conocido ataque cibernético que causó daños sea el que afectó el plan nuclear iraní al hacer ingresar un virus denominado "Stuxnet" que alteró los sistemas informáticos que controlaban a las centrifugadoras del programa de enriquecimiento de uranio (atribuido a EEUU e Israel). Otros ataques son producidos con fines de espionaje, como los que denunciaron países de Medio Oriente en el año 2012 por la introducción de un virus denominado "Flame" (también atribuido presumiblemente a EEUU e Israel), como los ataques que sufrió Estonia con bloqueos a sitios oficiales, bancos y medios a raíz de un conflicto con Rusia , o las permanentes denuncias de ataques recíprocos a nivel informático entre ambas Coreas (del Norte y Sur), China y los EE.UU, entre Pakistán e India, Rusia y Georgia y así otros tantos más. Fuente: "'Ciberamenazas': algo está cambiando", *El Mundo,* España, 21 de febrero de 2013.

(8) Declaraciones en su momento del subsecretario de Defensa de Estados Unidos, William J. Lynn III. Ver: "Ciberespacio: el nuevo ámbito de la guerra para el Pentágono", BBC, 27 de junio de 2011, *http://www.bbc.co.uk/mundo/movil/noticias/2011/07/110722_eeuu_pentagono_ciberespacio_estrategia_wbm.shtml*.

irrupción, legal e ilegal, a sistemas informáticos para la difusión de información (9).

Los hacktivistas buscan, a través de acciones específicas en el ciberespacio, lograr un alto impacto mediático o social.

- Alianza entre Estados y hackers

Las denominadas amenazas híbridas suelen ser ataques cibernéticos realizados por privados (hackers) pero patrocinados por un Estado. Suelen ser ataques directos a sistemas de defensa, de comunicaciones, pero también a través de tácticas de manipulación deliberada de la información/desinformación, como son las *fakes news,* para afectar a las instituciones, sistemas democráticos y los procesos electorales de los Estados (10).

- Organizaciones o grupos criminales

Tienen por objetivo obtener el rédito económico ilícito.

Pueden cometer dos tipos de delitos

1- Aquellos que solo pueden ser generados y perpetrados a través de dispositivos de Tecnologías de la Información y la Comunicación (TIC´s), en los cuales los dispositivos son tanto herramientas para cometer el delito como su objetivo mismo.

2- Aquellos ilícitos que son tradicionales cuya escala, alcance y magnitud se potencian y amplifican mediante el empleo de computadoras, redes, sistemas y cualquier otra TIC´s.

Entre las prácticas más usuales que realizan estas organizaciones se destaca el ingreso, mediante *malware*, en sistemas informáticos protegidos para obtener ganancias financieras; la incorporación subrepticia de algún virus que tome el control de un sistema informático y/o dispositivos determinados para luego solicitar sumas de dinero al usuario (persona y/o empresa) a cambio de su liberación; el acceso a datos personales sensibles; la generación de estafas electrónicas, etcétera.

El medio, los adelantos tecnológicos y nuevas estrategias, posibilita a los cibercriminales construir modelos de negocio altamente lucrativos y de bajo riesgo, encubriendo su accionar en lo dificultoso de marcar la trazabilidad de dichas operaciones pues suelen involucrarse a varias jurisdicciones.

Se advierte correctamente que "el empleo de nuevas modalidades de transacción financiera y económica, como las criptomonedas, para el tráfico y el comercio de bienes y prestación de servicios ilícitos o la extorsión, el fraude y la falsificación de medios de pago no monetarios, constituyen un serio desafío a la seguridad por su sofisticación y complejidad. Estos pueden ser utilizados en el blanqueo de capitales y la evasión de impuestos y representan una fuente de ingresos para el crimen organizado y por lo tanto son facilitadores de otras actividades como la financiación del terrorismo, que toma provecho de la dificultad de seguimiento que estas nuevas técnicas ofrecen" (11).

- Terroristas

Los ciberterroristas pueden efectuar acciones contra sistemas económicos/financieros, de defensa, salud y cualquier otra área estratégica y vital de un Estado.

También utilizan el ciberespacio como medio para realizar actividades propagandísticas para así fomentar la radicalización, reclutamiento y adiestramiento de individuos. Internet y las TICs pueden ser empleadas, además, para conseguir fondos para sus actividades, como un medio de intercomunicación y hasta como herramienta de divulgación sobre técnicas para la comisión de atentados.

(9) Dos claros ejemplos de hacktivismo son los grupos Anonymous y LulzSec.

(10) "Así fue la trama secreta de Rusia en las elecciones de Estados Unidos de 2016",*Clarín*, Argentina, 17 de diciembre de 2018, *https://www.clarin.com/mundo/trama-secreta-rusia-elecciones-unidos-2016_0_2vS7KMEsf.html*.

(11) Estrategia Nacional de Ciberseguridad de España (2019), aprobada por el Consejo de Seguridad Nacional. Referencia: BOE-A-2019-6347. *https://www.boe.es/eli/es/o/2019/04/26/pci487.*

- Desastres naturales

Pueden constituirse en una amenaza a la ciberseguridad pues sus consecuencias traen aparejados grandes daños a los sistemas informáticos en infraestructuras estratégicas (defensa, servicios, seguridad, salud, comunicación, etcétera).

V. Quiénes pueden ser afectados por un ciberataque

- Estados

Las amenazas en el campo cibernético pueden afectar áreas sensibles y críticas de un Estado. Pueden ser empleadas tácticas para desestabilizar a otros Estados afectando los sistemas de información y redes internas de la administración pública, economía, infraestructuras de telecomunicaciones, distribución de la energía, distribución de agua potable, transporte, defensa, salud, protección civil, etc., hasta la credibilidad en sus instituciones, líderes y regímenes políticos democráticos a través de campañas de desinformación (*fake news*) desplegadas en las redes sociales y otras plataformas.

- Empresas de bienes y servicios

Desde las grandes corporaciones hasta las pequeñas y medianas empresas pueden sufrir ataques en sus sistemas y redes informáticas. Las amenazas más frecuentes en cuestiones de ciberseguridad en el sector privado pueden englobarse en dos:

- *Amenazas intencionales*: Cuando el ataque cibernético lo produce, por ejemplo, un empleado que actúa por venganza ante una sanción laboral del empleador.

Amenazas accidentales. Producto de malas prácticas de un empleado mediante un obrar negligente que posibilita el ingreso de un virus que afectará el sistema informático.

- El Patrimonio Tecnológico

Como bien lo señala la Estrategia Nacional sobre Ciberseguridad de España (2019), se entiende como tal a todos "aquellos activos materiales o inmateriales que sustentan la propiedad intelectual e industrial del sector empresarial, que conforman nuestro presente y condicionan el desarrollo futuro".

Esta cuestión no es menor y hace a los recursos e independencia tecnológica de un país.

- Personas

Pueden ser afectadas también, pues utilizan internet en su quehacer diario al exponer, consciente e inconscientemente, sus datos personales.

VI. Definición de ciberseguridad

La ciberseguridad es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de una organización (pública o privada) y a los usuarios en el ciberentorno (12).

A su vez, todo sistema de ciberseguridad debe propiciar la protección de los siguientes ítems, a saber:

- la confidencialidad de los datos: impedir la divulgación de información a personas o sistemas no autorizados.

- la integralidad: lo que importa decir que los datos personales allí almacenados no puedan ser modificados o borrados por personal autorizado o no (intrusos/hacker), por un mecanismo extraño (virus), etcétera.

- la disponibilidad: lo cual significa que los datos personales deben encontrarse a disposición de quienes correspondan acceder a ellos, ya sean personas autorizadas, procesos o aplicaciones, siempre y cuando se respeten los protocolos y mecanismos de seguridad predispuestos con antelación, los cuales deben, por ende, estar desempeñándose correctamente.

Para que opere tal protección la ciberseguridad deberá contar con fases de prevención, localización y reacción ante la amenaza.

(12) *https://sites.google.com/site/jezabelydyddra/concepto.*

VII. Medidas que se implementan para la ciberseguridad

- Sector privado

Podemos aglutinar las diferentes medidas de seguridad que debe disponer toda base de datos en tres grandes grupos:

- *Las físicas*: recintos donde se almacenan las procesadoras de datos aptas para soportar cualquier eventualidad, como el caso de incendios, terremotos, explosiones, etc. Acceso mediante técnicas biométricas de personal solo autorizado para ingresar a estos recintos: exploración de retina, huellas dactilares, etcétera.

- *Las lógicas*: programas destinados específicamente para dotar de seguridad a estas bases para impedir accesos no autorizados. Ejemplos: cortafuegos, antivirus, restricciones de acceso mediante claves o sistemas de encriptación. También llevar registros de ingreso y egresos de las salas de almacenamiento/procesamiento, toda operatoria efectuada por su personal. Procedimientos para realizar *back up* (copias), etcétera.

- *El llamado "factor humano":* Importa básicamente instrumentar como medidas de seguridad una debida instrucción del personal autorizado de las bases de datos en su administración interna (lo que se debe hacer y aquello que no), conjuntamente con firmas de estrictos documentos concomitantes previos a su contratación, los llamados "Compromisos de confidencialidad", documentos que no solo están disponibles en las empresas del sector privado actualmente, sino que también en todas aquellas bases de datos públicas, como veremos más adelante en el presente trabajo. Este factor humano es, en muchos de los casos, la causa principal de pérdidas de datos personales, principalmente cuando provienen de errores involuntarios (por desconocimiento de los riesgos que importan ciertas prácticas en el manejo de los sistemas) o por motivos laborales estrictamente (ej., el estar descontento por su trabajo, mal pagos, etcétera).

- Sector estatal

Las mismas medidas en cuanto a la administración pública, servicios y empresas del sector, pero también son necesarias otras que hacen a la defensa nacional, donde ya es común observar la creación, dentro de las fuerzas armadas, de cuerpos específicos altamente capacitados en la ciberguerra, tanto en su faz defensiva como ofensiva.

También debe involucrar la instrucción sobre cuestiones de ciberseguridad de sus ciudadanos, como así también propiciar la capacitación permanente de su personal privado y estatal en todo lo atinente al manejo y empleo correcto de las modernas tecnologías de la comunicación e información.

VIII. Estrategias sobre ciberseguridad. Concepción.

a. Antecedentes internacionales

Ante amenazas ciertas y crecientes en el ciberespacio, distintos organismos internacionales y países han elaborado distintas estrategias para enfrentarlas.

Se ha definido a una Estrategia Nacional de Ciberseguridad como "un plan de acción nacional sobre la base de una visión nacional para lograr un conjunto de objetivos que contribuyan a la seguridad del ciberespacio" (13). Importan objetivos, prioridades, herramientas, creación de organismos específicos, procedimientos, concientización y capacitación sobre los riesgos en el ciberespacio, cooperación judicial/policial y de los sectores públicos y privados e internacional, medidas técnicas y legales, etc., las cuales deben alcanzarse dentro de un plazo determinado a los fines de establecer un marco adecuado en materia de ciberseguridad.

En toda Estrategia Nacional sobre Ciberseguridad están involucrados múltiples sectores: el gobierno, las agencias específicas, las fuerzas armadas y de seguridad, el sector industrial y comercial, las organizaciones de investigación y desarrollo, las universidades y la población en general.

Se tornaría muy extenso enumerar dichas iniciativas, por lo cual solamente enumeraré a modo ejemplificativo algunas de ellas. Como

(13) Luiijf, E. - Besseling, K. - De Graaf, P., "Nineteen National Cyber Security Strategies. International journal of critical infrastructures", 9 (1), ps. 3-31.

se podrá vislumbrar luego de su lectura, si bien con matices en cuanto al grado de su desarrollo, todos ellos encuentran rasgos similares.

b. Agenda de Ciberseguridad Global de la Unión Internacional de Telecomunicaciones

En virtud de las amenazas que acechan en el mundo virtual, la *Unión Internacional de Telecomunicaciones (ITU, International Telecommunication Union)* creó, en el año 2007, la *Agenda de Ciberseguridad Global (GCA - Global Cybersecurity Agenda),* cuya función básica es recrear dentro de la sociedad de la información un contexto que busque garantizar la confianza y seguridad en el uso de las Tecnologías de la Información y la Comunicación (TIC) mediante la cooperación internacional en materia de ciberseguridad.

Dicha Agenda busca, en pos de tal orientación, que los países que integran la ITU lleven a cabo la implementación de medidas legales, técnicas y de procedimiento, el establecimiento de estructuras organizacionales y la búsqueda de cooperación internacional en la materia.

A su vez, teniendo en cuenta si se adoptan o no tales parámetros se recrea un denominado "*Índice de Ciberseguridad Global (GCI, Global Cybersecurity Index)*", el cual tiene como objetivo medir y evaluar el compromiso de los países en la materia.

Desarrollado inicialmente en 2013, el GCI siempre está en constante actualización para determinar aspectos relevantes de la seguridad de los países miembros de la ITU.

c. EE. UU.

La cuestión de la ciberseguridad en un país de la importancia de los Estados Unidos es de suma relevancia y siempre han existido numerosas normativas internas sobre esta cuestión. Al respecto solo voy a mencionar en el presente trabajo a dos de las más recientes en sus rasgos que juzgo más relevantes.

Una de ellas fue dictada durante el segundo mandado de Barak Obama, en julio de 2016. Se trata de la "Directiva de Política Presidencial sobre Coordinación de Incidentes Cibernéticos de los Estados Unidos" *(Presidential Policy Directive United States Cyber Incident Coordination)* (14).

La misma reconoce y advierte expresamente que "el advenimiento de la tecnología en red ha estimulado la innovación, cultivado el conocimiento, fomentado la libre expresión y aumentado la prosperidad económica de la Nación. Sin embargo, la misma infraestructura que permite estos beneficios es vulnerable a actividades maliciosas, mal funcionamiento, errores humanos y actos de la naturaleza, lo que pone a la Nación y sus personas en riesgo. Los incidentes cibernéticos son un hecho de la vida contemporánea, y se están produciendo incidentes cibernéticos significativos con mayor frecuencia, que afectan a las infraestructuras públicas y privadas ubicadas en los Estados Unidos y en el extranjero" y que "si bien la gran mayoría de los incidentes cibernéticos se pueden manejar a través de políticas existentes, ciertos incidentes cibernéticos que tienen impactos significativos en una entidad, nuestra seguridad nacional o la economía en general requieren un enfoque único para los esfuerzos de respuesta. Estos incidentes cibernéticos importantes exigen la unidad de esfuerzos dentro del Gobierno federal y, especialmente, una estrecha coordinación entre los sectores público y privado".

La Directiva de Política Presidencial (PPD) establece los principios que rigen la respuesta del Gobierno Federal ante cualquier incidente cibernético, ya sea que este involucre a entidades gubernamentales o del sector privado.

Define y distingue claramente dos conceptos que son muy interesantes para resaltar:

- *Ciber incidente*: Es aquel evento que ocurre o se realiza a través de una red de computadoras que pone en peligro real o inminente la integridad, confidencialidad o disponibilidad de computadoras, sistemas o redes de información o comunicaciones, infraestructura física o virtual controlada por computadoras o sistemas de información, o información que reside en ellos.

(14) Presidential Policy Directive - United States Cyber Incident Coordination. PRESIDENTIAL POLICY DIRECTIVE/PPD-41, 26 de Julio de 2016, *https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident.*

Para los fines de esta directiva, un incidente cibernético puede incluir una vulnerabilidad en un sistema de información, procedimientos de seguridad del sistema, controles internos o implementación que podría ser explotada por una fuente de amenaza.

- *Incidente cibernético significativo*: Se parte de la probabilidad de que un incidente cibernético (o un grupo de incidentes cibernéticos relacionados) resulte en un daño demostrable para los intereses de seguridad nacional, las relaciones exteriores o la economía de los Estados Unidos o para la confianza pública, las libertades civiles o la salud pública y seguridad del pueblo estadounidense.

Para enfrentar estos desafíos se fijan una serie de principios rectores, destacándose el de la responsabilidad compartida donde los individuos, el sector privado y las agencias gubernamentales tienen un interés vital compartido, roles y responsabilidades complementarias para proteger a la Nación de la actividad cibernética maliciosa, como así también para gestionar los incidentes cibernéticos y sus consecuencias.

Además de la responsabilidad compartida en materia de ciberseguridad, se resalta que el gobierno federal dispondrá de las acciones necesarias para prevenir y reparar el ataque, fijándose quiénes se encargarán de los eventos, la coordinación entre las distintas entidades gubernamentales y el sector privado conjuntamente con otros Estados en virtud de las características del medio.

Se deja asentado que el gobierno federal determinará sus acciones de respuesta y los recursos que aporte basándose en una evaluación de los riesgos planteados para una entidad, la seguridad nacional, relaciones exteriores, la economía en general, la confianza pública, las libertades civiles o la salud y seguridad públicas de los americanos.

En septiembre del año 2018, se dio a conocer en los EEUU la "Estrategia Cibernética Nacional*" (National Cyber Strategy)* (15).

Dicha Estrategia se apoya en los siguientes pilares:

- *Protección*: tomar medidas específicas para resguardar las redes y la información federales, asegurar la infraestructura crítica, combatir la ciberdelincuencia y mejorar los informes de incidentes.

- *Promoción*: respaldar una economía digital promoviendo y protegiendo el desarrollo estadounidense en el sector. En este ítem se proyecta, fomenta y busca desarrollar una fuerza laboral en materia de ciberseguridad.

- *Se buscará identificar, contrarrestar, alterar, degradar y disuadir todo aquel comportamiento en el ciberespacio que sea desestabilizador y contrario a los intereses del país*: Se buscará la estabilidad cibernética a través de normas de comportamiento estatal responsable, detectando y responsabilizando por comportamiento inaceptable en el ciberespacio y la imposición de costos a los actores cibernéticos maliciosos.

En este sentido, no solo EEUU poseerá un rol de defensa, sino también ofensivo, con lo cual, ante un ataque informático de terceros (Estados, organizaciones terroristas y/o criminales, particulares patrocinados por Estados y hackers o grupos de estos), responderá en idéntico sentido.

- *Preservar la apertura a largo plazo, la interoperabilidad, la seguridad y la confiabilidad de Internet, al tiempo que se perseguirá respaldar el crecimiento del mercado para infraestructuras y tecnologías emergentes y crear capacidad cibernética a nivel internacional.*

d. Unión Europea

La Unión Europea ha emitido distintos documentos sobre ciberseguridad, entre los que se destacan:

- La *Estrategia de Ciberseguridad de la UE (Cybersecurity Strategy of the European Union)* del año 2013, en donde se busca recrear pautas para que el ciberespacio sea abierto, seguro y protegido, en donde se respeten los derechos de los ciudadanos de la unión dentro del entorno en línea.

(15) *https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.*

Fija una serie de pautas, a saber:

· Lograr la resistencia cibernética, aumentando las capacidades, la preparación, la cooperación, el intercambio de información y la sensibilización en el campo de la seguridad de las redes y de la información, para los sectores público y privado y a nivel nacional y de la UE;

· Reducir drásticamente el delito cibernético mediante el fortalecimiento de la experiencia de los encargados de investigarlo y enjuiciarlo, adoptando un enfoque más coordinado entre los organismos encargados de hacer cumplir la ley en toda la Unión y mejorando la cooperación con otros actores;

· Desarrollar una política y capacidades de la UE en materia de defensa cibernética en el marco de la política común de seguridad y defensa;

· Fomentar los recursos industriales y tecnológicos necesarios para beneficiarse del mercado único digital. Esto ayudará a estimular el surgimiento de una industria y un mercado europeos para las TIC seguras; contribuirá al crecimiento y la competitividad de la economía de la UE y aumentará el gasto público y privado en investigación y desarrollo (I + D)(16) sobre ciberseguridad;

· Mejorar la política internacional de la UE en materia de ciberespacio para promover los valores fundamentales de la UE, definir normas para un comportamiento responsable, promover la aplicación del derecho internacional existente en el ciberespacio y ayudar a los países fuera de la UE a desarrollar su capacidad de seguridad cibernética(17).

- Posteriormente, en el año 2015, la Comisión Europea ha presentado la *Agenda Europea de Seguridad para el período 2015-2020 (The European Agenda on Security)*(18). Consiste en una serie de medidas y herramientas concretas con el fin de contribuir a la cooperación de los Estados miembros en la lucha contra las amenazas a la seguridad y redoblar los esfuerzos comunes en la lucha contra el terrorismo y las amenazas a la seguridad, entre ellas la lucha contra la radicalización, el refuerzo de la ciberseguridad, la eliminación de las fuentes de financiación del terrorismo y la mejora del intercambio de información.

Si bien muchas iniciativas orientadas a dichos fines han sido puestas en práctica con resultados efectivos, aun resta implementar otras.

Por su parte, cada Estado posee sus propias estrategias en la materia bajo las directivas de la UE.

e. España

En España, se aplica desde el año 2013 la denominada *Estrategia de Ciberseguridad Nacional*, un documento elaborado por el Consejo de Seguridad Nacional que delimita todo lo concerniente en materia de seguridad en Internet que abarca a toda la administración pública, sector privado y a los ciudadanos. Dicho documento va recogiendo los aspectos más importantes sobre ciberseguridad con el fin de implantar de forma coherente y estructurada acciones de prevención, defensa, detección, respuesta y recuperación frente a las ciberamenazas.

En ese primer documento emitido se fija claramente la importancia vital de la ciberseguridad al advertir que "la multiplicidad de potenciales atacantes incrementa los riesgos y amenazas que pueden poner en graves dificultades los servicios prestados por las Administraciones Públicas, las Infraestructuras Críticas o las actividades de las empresas y ciudadanos. Además, existen evidencias de que determinados países

(16) I + D: investigación y desarrollo, abreviado I+D o I&D, (en inglés: *research and development*, abreviado R&D).

(17) Fuentes: "Communication on a Cybersecurity Strategy of the European Union – An Open, Safe and Secure Cyberspace. (Comunicación sobre una estrategia de ciberseguridad de la Unión Europea: un ciberespacio abierto, seguro y protegido)", 7 de febrero del 2013, *https://ec.europa.eu/digital-single-market/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security* y *https://ec.europa.eu/digital-single-market/en/news/communication-cybersecurity-strategy-european-union-%E2%80%93-open-safe-and-secure-cyberspace.*

(18) The European Agenda on Security, "Communication from the commission to the european parliament, the council, the european economic and social committee and the committee of the regions", Strasbourg, 28 de abril de 2015 COM(2015).

disponen de capacidades militares y de inteligencia para realizar ciberataques que ponen en riesgo la Seguridad Nacional. La ciberseguridad es una necesidad de nuestra sociedad y de nuestro modelo económico. Dada la influencia de los Sistemas de Información y Telecomunicaciones en la economía y en los servicios públicos, la estabilidad y prosperidad de España depende en buena medida de la seguridad y confiabilidad del ciberespacio, cualidades que pueden verse comprometidas por causas técnicas, fenómenos naturales o agresiones deliberadas".

Si bien la Estrategia de Ciberseguridad Nacional de España se va actualizando constantemente a tenor de nuevas amenazas, desafíos y estrategias que van surgiendo por el constante avance tecnológico, se han fijado originalmente seis objetivos específicos para cada sector. En líneas generales, ellos son:

1) Para la administración pública, garantizar que los Sistemas de Información y Telecomunicaciones utilizadas por estas poseen el adecuado nivel de seguridad y resiliencia (19);

2) Para las empresas y las infraestructuras críticas, se debe impulsar la seguridad y la resiliencia de las redes y los sistemas de información usados por el sector empresarial en general y los operadores de infraestructuras críticas en particular;

3) Buscar que, en el ámbito judicial y policial, entre otras medidas, se potencien las capacidades de prevención, detección, respuesta, investigación y coordinación frente a las actividades del terrorismo y la delincuencia en el ciberespacio. Se aboga por una mayor capacidad para la investigación y enjuiciamiento de los hechos ilícitos que correspondan, como así también fortalecer la cooperación judicial y policial internacional;

4) Campañas de sensibilización, concientizar a los ciudadanos, profesionales, empresas y a la administración pública de los riesgos derivados del ciberespacio;

5) Capacitación para alcanzar y mantener los conocimientos, habilidades, experiencia y capacidades tecnológicas que se necesitan para sustentar todos los objetivos en materia de ciberseguridad;

6) La búsqueda permanente de la colaboración internacional que contribuya en la mejora de la ciberseguridad, apoyando el desarrollo de una política de ciberseguridad coordinada en la Unión Europea y en las organizaciones internacionales, así como colaborar también en la capacitación de otros Estados que lo necesiten a través de las políticas de cooperación (20).

La nueva Estrategia Nacional de Ciberseguridad elaborada en el 2019 (21) fija la creación de un muy interesante Foro Nacional de Ciberseguridad, con el objetivo de que los sectores públicos y privados converjan y traten todas las cuestiones sensibles del área.

f. Argentina

Estrategia Nacional de Ciberseguridad. Decreto 829/2019

El *Decreto N° 577,* de fecha 28 de julio de 2017 (22), previó la creación del *Comité de Ciberseguridad* (23), el cual tuvo que elaborar la *Estrategia Nacional de Ciberseguridad*, apro-

(19) La resiliencia es la capacidad de adaptarse a un estado o situaciones adversas y la capacidad de recuperarse una vez superada la situación. La ciber-resiliencia debe ser entendida, entonces, específicamente como la capacidad para resistir, proteger y defender el uso del ciberespacio de los atacantes.

(20) *https://www.dsn.gob.es/es/estrategias-publicaciones/estrategias/estrategia-ciberseguridad-nacional.*

(21) Orden PCI/487/2019, del 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad Nacional. Referencia: BOE-A-2019-6347. https://www.boe.es/eli/es/o/2019/04/26/pci487.

(22) *http://servicios.infoleg.gob.ar/infolegInternet/anexos/275000-279999/277518/norma.htm.*

(23) Según el Decreto 577/2017 que creó el Comité, se establece que el mismo estará en la órbita del Ministerio de Modernización, y estará integrado por representantes del citado Ministerio, del Ministerio de Defensa y del Ministerio de Seguridad. (art. 1°).

Son tareas del Comité de Ciberseguridad:

a) Desarrollar la Estrategia Nacional de Ciberseguridad, en coordinación con las áreas competentes de la Administración Pública Nacional.

b) Elaborar el plan de acción necesario para la implementación de la Estrategia Nacional de Ciberseguridad.

bada posteriormente mediante la *Resolución 829/2019* (24).

Se ha argumentado correctamente que, en el marco del reconocimiento de las innumerables ventajas que traen aparejadas las TIC´s, también se debe hacer hincapié en sus aspectos negativos, entre ellos, los riesgos a la seguridad de las personas, las organizaciones y los gobiernos, estando el entorno digital amenazado por nuevas formas de delitos, la acción de grupos terroristas y la confrontación entre los Estados. Para ello, se requiere de estrategias globales que puedan enfrentar dichas amenazas.

La Estrategia Nacional de Ciberseguridad, establecida por el Poder Ejecutivo Nacional con el consenso del conjunto de la sociedad en forma multidisciplinaria y multisectorial, sienta los principios básicos y desarrolla los objetivos fundamentales que permitirán fijar las previsiones nacionales en materia de protección del Ciberespacio.

Su finalidad, menciona la Resolución 829/2019, es "brindar un contexto seguro para su aprovechamiento por parte de las personas y organizaciones públicas y privadas, desarrollando de forma coherente y estructurada, acciones de prevención, detección, respuesta y recuperación frente a las ciberamenazas, juntamente con el desarrollo de un marco normativo acorde".

Entre los argumentos para disponer de este plan, se destaca una cuestión que considero de suma importancia, como es la búsqueda de la protección de los datos e intimidad personales de los ciudadanos, ya que "atento el fuerte crecimiento de las empresas multinacionales que basan su negocio en la colección y el procesamiento de datos personales y que muchas veces tienen su sede y/o el despliegue de sus actividades en otras jurisdicciones, encontrándose por lo tanto sometidas a legislaciones foráneas, es necesario que la Republica Argentina tome debida nota de este fenómeno, a los fines de adoptar las medidas idóneas para proteger la privacidad de los datos de las personas y organizaciones de nuestro país." Destaca, además, que se advierten "graves amenazas y efectivos daños a los derechos de las personas y las organizaciones, en especial en lo referido a la privacidad de sus datos personales".

Esta cuestión antes señalada no es menor, pues va en sintonía con lo que dispone y advierte igualmente la Estrategia Nacional de Ciberseguridad de España (2019) cuando sostiene que "el análisis de los datos personales que circulan en la red se aprovecha para múltiples fines que abarca desde estudios sociológicos hasta campañas comerciales. El empleo malintencionado de datos personales y las campañas de desinformación tienen un alto potencial desestabilizador en la sociedad, y la explotación de brechas en los datos personales supone una violación a la seguridad de dichos datos, que afecta a la privacidad de las personas y a la integridad y confidencialidad de sus datos."

El plan diseñado prevé que la Estrategia Nacional de Ciberseguridad se sustenta e inspira en ciertos Principios Rectores, entre los que se destaca, claramente, el respeto por los derechos y libertades individuales, pues la protección de las personas en materia de ciberseguridad debe contemplar el respeto por los derechos y libertades individuales consagrados en la Constitución Nacional y en los Tratados Internacionales en los cuales la República Argentina sea parte.

Valoro, y mucho, que se haga hincapié sobre esta cuestión tan importante.

Además, los otros principios rectores de la Estrategia Nacional son:

- *Liderazgo*: Debe erigirse como un elemento central para promover detección, prevención y respuesta a incidentes cibernéticos, en coordinación con los estados provinciales, la Ciudad Autónoma de Buenos Aires, los municipios, el sector privado, el sector académico y la sociedad civil, con una adecuada articulación de las

c) Convocar a otros organismos para que participen en la implementación de medidas en el marco del plan de acción elaborado conforme lo establecido en el punto b) precedente.

d) Impulsar el dictado de un marco normativo en materia de Ciberseguridad.

e) Fijar los lineamientos y criterios para la definición, identificación y protección de las infraestructuras críticas nacionales. (art. 2°).

(24) RESOL-2019-829-APN-SGM#JGM. Ciudad de Buenos Aires, 24 de mayo de 2019.

competencias y recursos involucrados. Aplicar este principio es no solo necesario, sino imprescindible, desde mi opinión, para un correcto andamiaje en materia de ciberseguridad integral.

- *Integración internacional*: Los riesgos potenciales y todas las interrelaciones transfronterizas, que por el medio se canalizan, hacen que también opere la coordinación y cooperación con otros Estados.

- *Cultura de ciberseguridad y responsabilidad compartida*: Este principio rector conlleva que la ciberseguridad sea una cuestión integral entre todos los actores de la Nación: organizaciones públicas y privadas, académicas, la sociedad civil y la ciudadanía deban asumir las correspondientes responsabilidades para garantizar un Ciberespacio seguro. El Estado Nacional debe promover la generación de una cultura de ciberseguridad.

- *Fortalecimiento del desarrollo socioeconómico:* Se entiende que internet es un medio que potencia el desarrollo económico de distintos sectores por lo que, para llevar adelante dicho objetivo, se requiere necesariamente de una adecuada cobertura en materia de ciberseguridad.

El Plan elabora una serie de pautas, fomentando la capacitación y educación en materia de ciberseguridad, la cooperación entre sector público y privado, internacional, etc.

La Estrategia Nacional en materia de Ciberseguridad buscará potenciar además las capacidades de prevención, detección y neutralización de cualquier actividad maliciosa, contribuyendo a un ciberespacio seguro para quienes habitan nuestro país.

Objetivos de la Estrategia Nacional de Ciberseguridad

La Estrategia Nacional de Ciberseguridad traza los siguientes objetivos:

1. *Concientización del uso seguro del Ciberespacio*: implica fomentar que la cultura de la ciberseguridad se basa primeramente en el conocimiento adecuado sobre todos los riesgos que conlleva el empleo de las TIC´s.

2. *Capacitación y educación en el uso seguro del Ciberespacio*: para cumplimentar con el primer objetivo necesariamente se deberá hacer foco en la capacitación de los profesionales, técnicos e investigadores del área, entre otras medidas.

3. *Desarrollo del marco normativo*: un objetivo también fundamental será adecuar y generar las normas jurídicas, marcos regulatorios, estándares y protocolos para hacer frente a los desafíos que plantean los riesgos del ciberespacio, asegurando el respeto de los derechos fundamentales.

4. *Fortalecimiento de capacidades de prevención, detección y respuesta*: tanto la coordinación, cooperación y el fluido intercambio entre los distintos estamentos como el accionar de organismos de seguridad específicos cumplirán un rol importantísimo para lo cual será necesario promover las capacidades de los organismos y fuerzas de seguridad con competencia en la investigación y persecución de la delincuencia, el crimen organizado y el terrorismo en el ciberespacio.

5. *Protección y recuperación de los sistemas de información del Sector Público*: se requiere de altos niveles de protección y respuesta inmediata ante cualquier potencial riesgo y/o ataque informático, para lo cual debe ser prioridad la implementación correcta de sistemas de seguridad, su auditoría constante, flexibilidad en cuanto a la evolución tecnológica, etcétera.

6. Fomento de la industria de la ciberseguridad.

7. *Cooperación Internacional*: la promoción de la cooperación regional e internacional por las características de las TIC´s es ineludible en materia de ciberseguridad.

8. *Protección de las Infraestructuras Críticas Nacionales de Información*. para ello será necesario: promover la definición, identificación y protección de las infraestructuras críticas nacionales de la información; articular los esfuerzos públicos-privados para la construcción de capacidades de detección, resguardo y respuesta ante amenazas y ataques a partir de los recursos y responsabilidades de cada organización; fortalecer la cooperación en el intercambio de información ante vulnerabilidades y amenazas; promover esfuerzos coordinados dentro de las

redes industriales con el objetivo de fortalecer y resguardar los servicios críticos y productivos.

IX. Palabras finales

Mientras expongo y doy a conocer estas líneas, acciones silenciosas se libran en Internet, algunas de ellas sumamente peligrosas y dañinas, desplegadas tanto por personas, organizaciones criminales y/o terroristas, como por Estados, con múltiples objetivos, como ya fue señalado.

Del mismo modo, se libran acciones militares donde ya no solo se emplea el armamento tradicional, sino que pueden coexistir con otras invisibles a través de distintas tácticas, estrategias y ciberherramientas, todas con la suficiente capacidad para producir severos daños directos sobre los bienes, servicios, instituciones, formas de gobierno y hasta las personas indirectamente como ya fueran descriptas. Por ello, sin temor a equivocarme, considero que estamos transitando una nueva guerra fría, la cual se libra en el ciberespacio.

Todo este complejo contexto, donde cada vez existe una mayor interconexión y dependencia a las distintas tecnologías y los sistemas informáticos en toda área del quehacer humano, sobre todo en cuanto al funcionamiento de estructuras críticas esenciales como lo son la salud, el transporte, las finanzas, la energía, la defensa, etc., hace que ante cualquier potencial amenaza y/o ataque cibernético que estas pudieren sufrir se deba elevar todas aquellas medidas de protección imprescindibles para el resguardo de la confidencialidad, integridad o disponibilidad de la información almacenada en toda computadora, terminal o sistema informático.

Para que ello opere se requiere contar con un adecuado plan en materia de ciberseguridad para el cual se requerirá necesariamente de la participación conjunta y coordinada de una multiplicidad de actores que hacen a una Nación, sean estos públicos y privados, que conlleve una estrategia para enfrentar toda amenaza cibernética como la que aquí he comentado y que esta además sea erigida como política de Estado que perdure en el tiempo como una premisa central independientemente de los cambios políticos/ideológicos que conlleva cada gobierno.

Trazar una estrategia global e integrada donde se involucre al Estado en sus distintos niveles internos (nacional, provincial y municipal) en permanente coordinación y cooperación entre sí, y de este con otros Estados, organizaciones, universidades, proveedores de servicios de internet y las Tics hasta los usuarios de las mismas, sean del ámbito público (Gobierno, Fuerzas Armadas (25), Poder Judicial, Fuerzas de Seguridad, etc.) o del sector privado comprendido desde las grandes empresas multinacionales hasta cada uno de los ciudadanos.

La ciberseguridad de una Nación requiere que así ocurra, pues estamos protegiendo no solo la existencia y continuidad de la misma en la sociedad de la información, sino también sus áreas estratégicas y el resguardo de todos sus activos de información, tanto públicos como privados, conjuntamente con los datos personales de cada individuo que la habitan.

Es por ello que toda estrategia que se centre en la ciberseguridad nacional debe ser tratada, encauzada y aplicada con diligencia y suma responsabilidad, como así también deberá estar monitoreada constantemente para que opere una readecuación rápida que acompañe siempre con nuevas medidas los avances tecnológicos y los desafíos que irrogará la irrupción constante de nuevas prácticas maliciosas.

Debo señalar, finalmente, que las amenazas y los ataques en el ciberespacio ya son una realidad de magnitud inquietante y no meras conjeturas triviales ni cuestiones reservadas a la ciencia ficción literaria y a la industria audiovisual, por lo que merecen un privilegiado tratamiento como el que se intenta plasmar a través de una Estrategia Nacional de Ciberseguridad que debe ser una política de Estado, vuelvo a reiterar, pues lo que también está en juego es la defensa, ni más ni menos, que de nuestra soberanía como Nación.

(25) Nuestro país, en el año 2014, constituyó dentro del ámbito del Estado Mayor Conjunto (EMCO) el Comando Conjunto de Ciberdefensa al cual se le asignó la tarea de proteger la infraestructura crítica puesta bajo la órbita de la defensa. A su vez, el Ministerio de Defensa integra desde el año 2017 el Comité de Ciberseguridad Nacional, el cual elabora la Estrategia Nacional de Ciberseguridad.

Primeras reflexiones sobre el Derecho Fintech

MARINA BERICUA (*), **PABLO A. PALAZZI** (**) Y **SANTIAGO J. MORA** (***)

1. El presente artículo tiene como finalidad esbozar algunas primeras reflexiones vinculadas con el Derecho Fintech.

2. En primer lugar, debemos mencionar que a la denominación "Fintech" le atañe cierta problemática, por cuanto ella no posee contornos del todo definidos en la actualidad, por lo que no resulta completamente claro qué cuestiones deben quedar dentro y qué cuestiones deben quedar fuera de la materia bajo estudio.

En este contexto, en un extremo podemos encontrar definiciones muy amplias que entienden que dicha denominación incluye todas aquellas actividades que impliquen el empleo de la innovación y los desarrollos tecnológicos para el diseño, oferta y prestación de productos y servicios financieros (1). Esta posición resulta consistente con el hecho de que la palabra *fintech* está formada por la contracción de las palabras anglosajonas *financial* y *technology* ("tecnología financiera", en español). En ese marco, la materia incluiría a los siguientes actores principales: *(i)* entidades financieras tradicionales (incluyendo bancos puramente digitales); *(ii)* nuevas empresas que comienzan a competir con las entidades financieras tradicionales en distintos verticales del negocio financiero; y *(iii)* compañías que solo pretenden realizar desarrollos tecnológicos y prestar servicios a las empresas anteriores.

En el otro extremo, podemos encontrar posiciones más restrictivas que entienden que no corresponde incluir en la materia Fintech el resultado de todo uso de la tecnología por parte del sector financiero, dado que dicho uso viene sucediendo desde hace décadas mientras que el concepto de Fintech es mucho más novedoso. Dichas posiciones entienden más relevante la revolución tecnológica que sucedió en los últimos años y que ha permitido a empresas distintas de las entidades financieras tradicionales comenzar a competir con estas últimas en diversos verticales del negocio financiero, por

(*) Abogada por la Universidad de Buenos Aires. LL.M. por Columbia University School of Law. Directora de la Maestría en Derecho Empresario del Departamento de Derecho y Directora de Legales de la Universidad de San Andrés.

(**) Master en Derecho de Fordham University. Es Profesor de Derecho en la Univ. de San Andrés y Director del Programa de Derecho de Internet de la misma Universidad, y codirector del CETYS de UDESA.

(***) Abogado y magíster en Derecho & Economía. Docente de la materia "Elementos de Derecho Comercial" (UBA) y de la materia "Fintech" en la Universidad de San Andrés. Investigador en el Centro de Estudios de Tecnología y Sociedad (CETYS) de la Universidad de San Andrés. Integrante de la Mesa de Innovación Financiera del Banco Central de la República Argentina. Miembro de la ONG Bitcoin Argentina.

(1) Ver, p. e., Asociación Española de FinTech e InsurTech (AEFI), *Libro Blanco de la Regulación FinTech en España*, octubre de 2017 [http://bit.ly/2ZsIyLk].

lo que acotan el ámbito de la materia a las actividades de esas empresas (2).

Sin pretender tomar posición en la discusión mencionada, nosotros llamamos "empresas fintech" a aquellas empresas que comienzan a competir con las entidades financieras tradicionales en distintos verticales del negocio financiero; esto, por cuanto consideramos que dicha referencia es la que se ha adoptado en los incipientes usos y costumbres de nuestro país. Sin embargo, aclaramos que no pretendemos con ello limitar el ámbito de la materia.

3. En cualquier caso, sea cual fuere la posición que se adopte, todas ellas coinciden en que, en el marco de este fenómeno Fintech, se generaría una serie de beneficios muy importantes para la sociedad, a saber: *(i)* un incremento en la innovación, tanto en la creación de nuevos modelos de negocios como en la reformulación en la forma de operar de los productos y servicios financieros preexistentes; *(ii)* un aumento de la competencia y una disminución en las fallas de mercado que pudieran existir (como, por ejemplo, abusos de posición dominante, asimetrías de información, etcétera); *(iii)* una simplificación funcional y una desintermediación operativa; y *(iv)*, como consecuencia de lo anterior, se obtendrían distintos tipos de eficiencias, disminuciones de costo, adaptaciones a las necesidades de los usuarios e inclusión financiera (lo cual significa que más usuarios puedan incorporarse al sistema).

4. Otro aspecto principal que debe tenerse en cuenta sobre la materia es la diferencia que en principio existe entre la actividad de las tradicionales entidades financieras y aquella que desarrollan las distintas empresas fintech, así como la diferencia entre los riesgos derivados de cada tipo de actividad.

Las entidades financieras tradicionales llevan adelante lo que se identifica como intermediación habitual entre la oferta y la demanda de recursos financieros, actividad que conlleva una serie de riesgos muy importantes que han sido debidamente delimitados en base a muchos años de estudio. En la mayoría de los casos, las empresas fintech llevan adelante negocios puntuales y específicos, por los cuales se pueden vincular con demandantes de recursos financieros o con oferentes de recursos financieros, pero no intermediando de manera habitual entre ambos. Las actividades de las empresas fintech también pueden conllevar riesgos, pero en principio no serían los mismos riesgos que conlleva la actividad de las tradicionales entidades financieras. Adicionalmente, dichos riesgos pueden ser distintos entre sí dependiendo del vertical de la industria fintech del que se trate. Sobre el particular, además, se menciona que en muchos casos los riesgos correspondientes a los distintos negocios fintech pueden no encontrarse del todo identificados, analizados y cuantificados aún, máxime cuando en muchos casos los negocios en cuestión pueden todavía estar en un estado incipiente al ser solo proyectos de negocios o por no haberse desarrollado del todo aún.

El principio general mencionado no quita que puedan llegar a existir proyectos fintech específicos (actuales o futuros) que efectivamente realicen una actividad asimilable a la de las tradicionales entidades financieras, debiendo en ese caso establecer, caso por caso, la necesidad y conveniencia de que para su establecimiento y desarrollo se cumplan los estándares regulatorios aplicables a dichas tradicionales entidades financieras.

5. En este contexto, en razón de la novedad de los negocios involucrados, la tensión con las estructuras preexistentes y los beneficios que se generarían con el desarrollo de la materia, se presenta una serie de particularidades vinculadas con la regulación de la materia Fintech que someramente se describen a continuación.

(a) En primer lugar, se observa que muchos reguladores, en muchos países, han entendido que la promoción de estos negocios es una "cuestión de Estado".

En el derecho comparado se menciona al Reino Unido como el país que más rápido se posicionó como un promotor de la innovación en el sector financiero. En particular, a través de la *Financial Conduct Authority* (FCA), que en

(2) Ver, p. e., World Economic Forum, "Beyond Fintech: A Pragmatic Assessment Of Disruptive Potential In Financial Services", agosto de 2017 [http://bit.ly/2Zl9bmp].

2014 lanzó el llamado *Project Innovate*, dentro del cual implementó lo que se dio en llamar los *Regulatory Sandboxes*, el *Request Direct Support* y las *Advice Units* (3). Luego de esta primera experiencia, muchos otros países de Europa y del resto del mundo buscaron seguir los pasos del regulador británico.

Como otro ejemplo de la importancia de las fintech para los Estados, en Europa se observa un importante impulso en desarrollar el potencial de la tecnología *blockchain*. En este sentido, el 1 de febrero de 2018 la Comisión Europea lanzó el Observatorio y Foro Blockchain de la UE, que tiene como objetivos mapear iniciativas clave, monitorear desarrollos e inspirar acciones comunes, entre otros. Asimismo, y en el mismo ámbito, el 10 de abril del mismo año se firmó una declaración para crear la Asociación Europea de Blockchain (*European Blockchain Partnership*, EBP) y cooperar en el establecimiento de una Infraestructura de Servicios Europea de Blockchain (*European Blockchain Service Infraestructure*, o EBSI) que apoyará la prestación de servicios públicos digitales transfronterizos con los más altos estándares de seguridad y privacidad (4).

(b) A pesar de que ciertos reguladores han demostrado que estos nuevos negocios tienen importancia para sus Estados, otros reguladores han demostrado no ser necesariamente consistentes entre sí.

En este sentido, puede suceder por ejemplo que en un país determinado la autoridad monetaria quiera flexibilizar la normativa de *onboarding* digital pero la autoridad que lucha contra el lavado de dinero quiera reforzar los regímenes de identificación de clientes. Además, al surgir nuevos negocios (que por definición serán atípicos, es decir, no regulados por la normativa vigente), cada organismo público posiblemente quiera analizar su naturaleza jurídica en función de su propia visión y sus propios intereses y competencias, lo cual podrá derivar en resultados no coordinados, generando tensiones y rispideces. Todo esto, sin siquiera analizar que muchas veces se generarán distorsiones y desincentivos adicionales mediante disposiciones en materia impositiva, en tanto quien redacta la regulación en dichos casos tiene como objetivo principal el de recaudar, sin conocer necesariamente el impacto que sus medidas pueden generar en estos negocios.

Los inconvenientes derivados de las inconsistencias y desalineación de objetivos se potencian por el carácter regional o internacional de muchos de estos emprendimientos, con lo que los promotores de estos negocios no solo tendrán que analizar las posibles discrepancias y conflictos en el país de lanzamiento, sino también en el resto de los países en los que la empresa quiera operar y las asimetrías que pudieren existir entre las regulaciones de los distintos países.

(c) No solo se observan discordancias entre reguladores, sino también entre los mismos privados involucrados o relacionados.

En este sentido, es importante mencionar que el sector privado no tiene una posición única respecto de los aspectos regulatorios de la presente materia, ya que existen posturas que sostienen que conviene avanzar con regulaciones complementarias a las existentes, posturas que sostienen que debe aplicarse la normativa vigente, posturas que sostienen que debe avanzarse con la desregulación (o desmantelamiento) de las normas existentes y posturas que sostienen que solo debería existir y desarrollarse una autorregulación.

Además, dentro de cada posición, los privados también pueden sostener diferentes opiniones o perseguir diferentes fines. Por ejemplo, dentro de los privados que proponen alguna forma de regulación, están aquellos que proponen regular a los nuevos actores tal como están regulados los actores tradicionales y los que resaltan que los riesgos que soportan estos nuevos actores son distintos de los riesgos de los actores tradicionales, por lo que se los debe regular de una manera distinta que permita contener dichos riesgos específicos. En el mismo contexto, están las empresas ya consolidadas (tanto tradicionales como nuevas) que quizás busquen generar barreras de entrada para restringir el acceso de otras empresas que puedan competir con ellas, los que sostienen que la regulación debería

(3) Ver: http://bit.ly/2zmoewB.

(4) Ver: http://bit.ly/2NtAS4Z.

funcionar como un *stopper* para que los actores consolidados no obstaculicen el ingreso y operación de jugadores adicionales, las empresas fintech que necesitan la regulación como forma de validación por parte del Estado para lograr inversiones o financiamiento externo, etcétera.

Asimismo, dentro de los privados que entienden que no es necesario regular están los que se guían por razones filosóficas que entienden a cualquier regulación como una intromisión del Estado en las libertades de las personas, los que se guían por el entendimiento de que hasta que los nuevos negocios no tengan determinado volumen no puede saberse a ciencia cierta la medida del riesgo que conllevan (y la convicción de que su regulación anticipada solo logrará obstaculizar su desarrollo) y los que entienden que este tipo de negocios evolucionan constantemente (con lo cual, incluso aunque se lograra definir una regulación perfecta en un momento determinado, esta quedaría indefectiblemente desactualizada rápidamente). En este contexto, además, están los que observan que, en ámbitos específicos como el de las criptomonedas, resulta especialmente complejo pretender regular de la manera tradicional en tanto no existe en el caso un administrador central y por eso es muy difícil realizar el monitoreo e imponer una sanción en caso de incumplimiento, etcétera.

(d) Una cuestión adicional que complejiza el presente análisis es —conforme ya lo hemos mencionado— el hecho de que la materia Fintech no incluye un único modelo de negocio, sino que hay muchos "verticales" involucrados y cada uno se encuentra regulado en la actualidad con una base normativa distinta (aunque los negocios novedosos sean atípicos, el derecho vigente de todos los países igualmente se aplicará a ellos; ello, teniendo en cuenta las normas que regulen negocios preexistentes similares o los riesgos que se activen en el caso concreto), cada uno tiene necesidades distintas para desarrollarse y cada uno genera riesgos distintos para el interés público.

6. Hemos dicho en reiteradas oportunidades que la Argentina se encuentra en un destacado lugar en el ecosistema fintech regional y mundial, teniendo en cuenta el valor y la creatividad de los emprendedores locales y la calidad de los proyectos que están desarrollando. Además, hemos dicho también que los potenciales beneficios de este tipo de negocios parecen en particular relevantes y útiles para nuestro país, que especialmente necesita competencia, innovación, simplificación de procesos y descentralización. Se presenta así una importante oportunidad y el enorme desafío de potenciar y aprovechar este fenómeno de la mejor manera posible.

En este contexto, reiteramos que cualquiera sea el enfoque regulatorio que se adopte en nuestro país (regulación, no regulación, autorregulación o desregulación) es necesario que el proceso sea resuelto y encarado como un proceso colectivo que involucre a todos los interesados.

Cualquier proceso regulatorio (incluso aquel en el que se discuta la conveniencia de la eliminación o falta de regulación) debería hacerse con la participación de todos los reguladores interesados, todo el espectro del sector privado (incluyendo a las empresas de todos los tamaños y a las empresas que aún no han comenzado a operar), la sociedad civil en representación de los intereses de los consumidores y la academia. Este trabajo, desde ya, debería también hacerse vertical por vertical, descartando en principio la posibilidad de elaborar enfoques generales a modo de "ley fintech" que no permitan contemplar las particularidades de cada tipo de actividad y los riesgos que cada tipo conlleva, siempre teniendo en cuenta, por supuesto, la necesidad de armonización entre las distintas regulaciones.

¿Cómo nos afectará Libra? Un análisis de la Criptomoneda de Facebook

FERNANDO O. BRANCIFORTE (*)

I. Introducción

El título del presente artículo podría referirse a una de las tantas predicciones de los astros y horóscopos que abundan en las diversas revistas, pero lo que nos proponemos analizar en el presente es cómo influirá en nuestras vidas la moneda que pretende lanzar Facebook al mercado, cuya denominación es "Libra".

Si hemos leído y escuchado en infinidad de oportunidades que vivimos en un mundo tecnológico donde la tecnología gobierna nuestras vidas, también debemos ser conscientes que la economía es otro de los factores que nos influyen en nuestro andar.

Nos gusten u odiemos las matemáticas; entendamos mucho, poco o nada de economía, lo cierto es que en el mundo actual, para adquirir bienes y servicios, debemos recurrir a la misma y hacer uso de las monedas locales.

Y es en este mundo económico y tecnológico donde, un grande de las comunicaciones como es Facebook, ha visto la necesidad de crear lo que podemos llamar una "tecnología económica" y otorgar acceso a este "nuevo mundo" a aquellas personas que están fuera del sistema financiero.

Fue así que, el 18 de junio de 2019, el CEO de Facebook, Mark Zuckerberg, le manifestó al público la creación de "Libra" y sus intenciones respecto a que la misma esté completamente operativa y en funcionamiento para mediados del 2020.

Inmediatamente los grandes gobiernos del mundo y los principales bancos, quizás por temor o desconocimiento, comenzaron a criticar duramente este movimiento del gigante de las comunicaciones a tal punto que David Marcus, director ejecutivo del proyecto, tuvo que presentarse ante el Comité Financiero del Senado de los Estados Unidos para defender a "Libra".

¿Por qué generó tanto ruido en el mundo esta criptomoneda existiendo tantas a la fecha? ¿Qué la hace diferente? ¿Es realmente peligrosa? Y, finalmente, ¿cómo puede afectar a nuestra legislación y a nosotros mismos como usuarios y operarios del derecho? Serán preguntas que intentaremos responder, o al menos analizar, en el presente ensayo.

II. Un poco de historia

Antes de entrar de lleno en el análisis propuesto debemos hacer un poco de historia, ver cómo fueron evolucionando las ideas y los diversos proyectos que trajeron a Libra hoy a la vida.

(*) Miembro de la Comisión Directiva del Instituto de Derecho del Consumidor del Colegio de Abogados de Bahía Blanca; Miembro del Instituto de Derecho Informático y TICS del Colegio de Abogados de Bahía Blanca.

Si bien las criptomonedas como hoy las conocemos comenzaron a gestarse en el año 2008 con causa en la crisis financiera de los Estados Unidos, lo cierto es que el concepto o idea de criptomoneda fue descripta por primera vez por Wei Dai, en 1998, donde se propuso la idea de crear un nuevo tipo de dinero descentralizado que usara la criptografía como medio de control.

Prestando atención a nuestra vida diaria, podemos observar que las criptomonedas no son una novedad digital. Desde hace varios años y, aún en el presente, usamos dinero digital para hacer todo tipo de transacciones desde tarjetas de crédito, débito, envíos, etc. Todo depende de la confianza del emisor y receptor.

Sin embargo, el concepto en sí de "criptomoneda" se refiere a un capítulo mayor, este hace referencia a la capacidad de utilizar un sistema de criptografía capaz de brindar seguridad y confianza continua.

Los primeros intentos de vincular la criptografía con el dinero fueron realizados por el criptógrafo David Chaum, quien en 1983 concibió un sistema criptográfico monetario electrónico llamado eCash. Más tarde, en 1995, implementó DigiCash, que utilizaba la criptografía para volver anónimas las transacciones de dinero, aunque con una emisión y liquidación (pago) centralizado (1). Este sistema requería un software para retirar dinero de un banco y designar claves cifradas específicas antes de que puedan enviarse a un destinatario. Esto permitió que la moneda digital no fuera rastreable por el banco emisor, el gobierno o cualquier tercero. Sin embargo, sus sistemas no generaron la confianza necesaria y no funcionaron.

En 1996, la NSA publicó una investigación titulada "How to make a Mint: the Cryptography of Anonymous Electronic Cash" (2). Esta investigación describía un sistema de criptodivisa, publicada en una lista de correo del MIT9. Más tarde, en 1997, fue publicada en *The American Law Review* (Vol. 46, Issue 4) (3).

Si bien las ideas estaban, la realidad es que para aquella época no existía, o al menos aún no estaba desarrollada, la tecnología necesaria para llevarlas adelante.

No fue sino hasta el año 2008 cuando un grupo de personas bajo el pseudónimo Satoshi Nakamoto deciden crear un protocolo de red descentralizada, accesible a todo el público, con capacidad de verificación también descentralizada y completamente segura por su sistema criptográfico.

Un año después, se crea la famosa criptomoneda denominada "Bitcoin", la cual recién se comienza a utilizar en el año 2010.

Ahora bien, este sistema creado por Nakamoto es conocido como "tecnología Blockchain" o "cadena de bloques".

Básicamente, "Blockchain" es una cadena de bloques interconectados entre sí (4).

Para entender al sistema Blockchain debemos imaginar una cadena donde cada bloque es un libro contable que está encriptado y enlazado al bloque siguiente, de modo tal que no se puede modificar uno sin afectar al otro.

Asimismo, cada bloque o libro contable va a estar replicado en todo el sistema de nodos (computadoras distribuidas en todo el mundo). Esto genera una característica de publicidad por lo que cualquier operación y bloque va a ser visible en todos los nodos miembros del blockchain, de modo que, si algo se modifica en un nodo, en los otros 3, por ejemplo, seguirá diferente, lo cual también le da carácter de seguridad, ya que una vez ingresado el dato no se podrá borrar si no hay consenso de todos.

Así vemos otra característica que es la descentralización, no hay un ente central que

(1) Chaum, David, *"Blind signatures for untraceable payments". Advances in Cryptology Proceedings of Crypto*, 1983, (en inglés) 82 (3): 199-203.

(2) *http://groups.csail.mit.edu/mac/classes/6.805/articles/money/nsamint/nsamint.htm.*

(3) Law, Laurie; Sabett, Susan; Solinas, Jerry, "*How to Make a Mint: The Cryptography of Anonymous Electronic Cash", American University Law Review*, 1997, 46.

(4) *https://www.xataka.com/especiales/que-es-blockchain-la-explicacion-definitiva-para-la-tecnologia-mas-de-moda.*

establezca las reglas, sino que el sistema se maneja por consenso de todos los nodos.

A efectos de una mayor interpretación del sistema Blockchain nos remitimos a nuestra anterior publicación titulada "Las nuevas tecnologías y el Derecho" (5), así como a la publicación realizada por el Dr. Santiago J. Mora titulada "La tecnología *blockchain*. Contratos inteligentes, ofertas iniciales de monedas y demás casos de uso" (6), en las cuales se explica aún más detalladamente el funcionamiento de este sistema.

De este modo, se creó un nuevo sistema, descentralizado, capaz de ser utilizado como medio de pago y con infinidad de funciones, las cuales hasta hoy siguen siendo desconocidas.

Con el correr de los años, la masividad de Bitcoin generó que se fueran creando otros sistemas y variantes y, con ello, gran cantidad de criptomonedas que existen a la fecha.

III. ¿Qué es una criptomoneda?

Para continuar con el análisis y descubrir qué es lo que realmente nos ofrece Facebook, debemos definir primero criptomoneda.

Actualmente no existe la definición de criptomoneda en el diccionario de la Real Academia Española.

El diccionario de Oxford incluyó su definición en inglés *cryptocurrency* estableciendo que es: "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".

El diccionario de Cambridge, por su parte, la ha definido como: "Una moneda digital producida por una red pública en lugar de cualquier gobierno, que utiliza la criptografía para asegurar que los pagos se envían y reciben de forma segura" (7).

Finalmente, Wikipedia la define como: "Un medio de intercambio que utilizan la criptografía para asegurar las transacciones y controlar la creación de nuevas unidades" (8).

Más allá de la definición que le otorguemos, lo que debemos tener en cuenta es que las características principales de toda criptomoneda son su seguridad brindada por su sistema criptográfico, así como su descentralización y confianza que brinda la tecnología *blockchain* en la cual se basen.

Como manifestamos en la anterior publicación, para poder adquirir o realizar transacciones de criptomonedas, la persona debe tener una billetera virtual o *wallet* que es donde se alojarán las criptomonedas. A la misma se accede por medio de una clave privada y una clave pública del *blockchain* que hará una doble verificación.

De este modo, se accederá a nuestra *wallet* donde se ordenará la transferencia de x cantidad de criptomonedas, esa información se anotará en un bloque del *blockchain*, será verificado por todos los nodos de que el monto que yo quiero transmitir es el correcto y que no es más que el que tengo (recordemos que al ser una cadena de bloques todas las informaciones están concatenadas con lo cual si en un bloque anterior pasé a tener 3 criptomonedas, en este bloque esta información estará cargada y no voy a poder transmitir más de 3 criptomonedas), producida la verificación se transmite y se escribe el nuevo bloque donde tendré 0 criptomonedas si es que transmití los 3 que tenía.

Así, las diferentes criptomonedas creadas desde el 2008 fueron generadas con diversos fines que van desde medio de pago (el fin del *Bitcoin*) hasta sistemas bases de Smarts Contracts (Red Etherum y su criptomoneda Ether).

(5) Branciforte, Fernando O., "Las nuevas tecnologías y el Derecho", La Ley, 22/07/2019.

(6) Mora, Santiago J., "La tecnología *blockchain*. Contratos inteligentes, ofertas iniciales de monedas y demás casos de uso", La Ley, 1/04/2019.

(7) *https://www.oroyfinanzas.com/2014/10/que-es-criptomoneda/.*

(8) *https://es.wikipedia.org/wiki/Criptomoneda#cite_note-11.*

Por otro lado, dada su cualidad de ser descentralizadas, generó que su valor dependa exclusivamente de la oferta y la demanda, es decir, de su comercio.

Ello, a su vez, trajo como consecuencia uno de sus mayores defectos, la alta volatilidad de su valor.

Tan es así que el BCRA en una de sus circulares estableció que es un bien riesgoso sin base monetaria. Y yendo aún más con la última modificación a la CNV, la misma establece que en bienes como las criptomonedas habrá que recurrir a fondos comunes de inversión que serían los expertos a la hora de invertir (9).

Por otro lado, a nivel internacional, ya se han generado diversas cuestiones en base con las criptomonedas que tienen como núcleo principalmente al *Bitcoin*.

Al solo efecto informativo, ya que no es el sentido del presente artículo, podemos manifestar que la Sala de lo Penal del Tribunal Supremo de España ha dictado Sentencia con fecha 20 de junio de 2019, en el Recurso de Casación 998/2018 donde aborda efectos de responsabilidad civil del *Bitcoin* entrando a analizar la naturaleza legal de esta criptomoneda.

En la Sentencia nº 326/2019 (10), con fecha del 20 de junio, el Tribunal Supremo confirmó la dictada por la Audiencia Provincial de Madrid que por primera vez en España establecía una condena por un caso de estafa con *bitcoins*.

La sentencia del Tribunal Supremo señala que "el acto de disposición patrimonial que debe resarcirse se materializó sobre el dinero en euros que, por el engaño inherente a la estafa, entregaron al acusado para invertir en activos de este tipo" y resalta que la criptomoneda "no es algo susceptible de retorno" al no considerarlo dinero legal ni objeto material.

Dicho Tribunal manifiesta su propio concepto de criptomoneda al definirlo como "un activo patrimonial inmaterial, en forma de unidad de cuenta definida mediante la tecnología informática y criptográfica, cuyo valor es el que cada unidad de cuenta o su porción alcance por el concierto de la oferta y la demanda en la venta de estas unidades se realice a través de las plataformas de trading".

IV. ¿Qué es Libra? ¿Cuál es su función?

Hasta aquí hemos visto la evolución de las criptomonedas, su origen y su posible concepto. Ahora pasaremos a analizar puntualmente a Libra. Para ello, debemos recurrir al *White Paper* de la misma (11).

Para aquellos que no están familiarizados con el concepto de *White Paper* podemos decir que es un documento que incluye un resumen de un problema que el proyecto está tratando de resolver, la solución a ese problema, así como una descripción detallada de su producto, su arquitectura y su interacción con los usuarios (12).

Pasándolo a nuestro plano terrenal podemos asimilar el *White Paper* a un estatuto o carta de fundamentos de su creación.

Ahora bien, si analizamos puntualmente el *White Paper* de Libra observamos que allí se establece como objetivo el crear una nueva *blockchain* descentralizada capaz de contener una criptomoneda de baja o nula volatilidad y una plataforma capaz de crear contratos inteligentes.

Los creadores de Libra ven en su sistema *Blockchain* una forma de solucionar los problemas de falta de financiamiento de la población.

Asimismo, son conscientes de que la gran volatilidad de las criptomonedas aleja a la gente de la misma. Es así que deciden establecer un nuevo carácter de criptomoneda.

Para ello, a través de Libra, se intenta establecer un sistema financiero moderno, *on line*, sencillo, intuitivo y accesible para todos aquellos que tengan un medio móvil.

(9) *http://www.cnv.gob.ar/Advertencias/Notas/Oferta%20Inicial%20de%20Monedas%20Virtuales.pdf.*

(10) *https://www.maestreabogados.com/wp-content/uploads/2019/07/supremo-estafa-bitcoins.pdf.*

(11) *https://libra.org/es-LA/white-paper/.*

(12) *https://es.cointelegraph.com/ico-101/what-is-a-white-paper-and-how-to-write-it.*

La criptomoneda Libra se crea en tres bases:

1. Una nueva, segura y propia *Blockchain* de un solo bloque;

2. Un respaldo de valor

3. Ser gobernada por una asociación independiente llamada "Asociación Libra" que tendrá como función ir mejorando el ecosistema de Libra en base a los beneficios de los usuarios.

La estructura de la *Blockchain* Libra es diferente a la de las otras *Blockchain*. Estas últimas tienen un sistema que podríamos llamar como una colección de transacciones en varios bloques. Mientras que *Blockchain* Libra es una sola estructura, podríamos decir un solo bloque, que tiene todo el historial de las transacciones que se van produciendo. Se simplifica así la posibilidad de acceder a datos remotos y se consigue mayor velocidad de transferencia de datos.

Esta nueva *Blockchain* permitirá crear uno o varios seudónimos con los cuales se mantendrá el anonimato típico de las transacciones de criptomonedas.

La principal característica del *Blockchain* Libra es que, en un comienzo, los nodos deben ser autorizados por la Asociación Libra, se piensa en un futuro que sea de libre acceso.

Por otro lado, esta Blockchain será de código abierto, esto significa que cualquiera puede hacer uso del código para crear diferentes sistemas sobre el mismo, como por ejemplo, Smart Contracts que usen como núcleo a Libra.

Siguiendo con el análisis, observamos que se crea la Reserva Libra que estará vinculada a la criptomoneda para darle una vinculación de valor de modo tal que su volatilidad sea minúscula en comparación con el resto de las criptomonedas hoy existentes.

La Reserva Libra será administrada por la Asociación Libra para mantener un valor coherente de la moneda.

Los miembros fundadores de la Asociación Libra están distribuidos por todo el mundo y convergen en diferentes actividades como son las financieras, tecnológicas, telecomunicaciones, *blockchain*, capitales, etcétera.

Entre los miembros más destacados vemos a PayPal, Visa, MasterCard, Mercado Pago, Spotify, EBay, Vodafone, Anchorage, Coinbase, Union Square, Venture, Alastria, entre otros.

Por parte de Facebook se creó Calibra, como una subsidiaria de esta, y encargada específicamente del sector financiero.

Todos los miembros de la Asociación, incluyendo Facebook, tendrán los mismos derechos y obligaciones.

Con estas características, Libra fue creada para ser una criptomoneda digital estable, que tenga un seguro por medio de una reserva vinculada a un tipo de moneda real (en contraposición con la moneda virtual) y con el apoyo de varias casas de cambio competitivas que permitan el comercio de Libra de forma segura.

Así se permite que cualquier persona que adquiera esta criptomoneda pueda, en cualquier momento, cambiarla por la moneda fíat (billete real) como si cambiásemos de monedas en un viaje internacional.

Para intentar mantener un valor estable, Libra será respaldada por monedas de baja volatilidad, así como depósitos bancarios y títulos valores de corto plazo colocados en diversos bancos del mundo.

Esto no quiere decir que Libra estará vinculada en precio a una moneda, tendrá volatilidad, pero se intentará que esta sea mínima y que esté relacionada con el valor de los activos elegidos como respaldo.

El interés y la ganancia que generen estos activos se utilizarán para cubrir los costos del sistema, garantizar tarifas de transacción bajas, pagar dividendos a los miembros fundadores de la Asociación Libra, etcétera.

Todas las decisiones acerca de este nuevo ecosistema y del funcionamiento de Libra serán realizadas por los miembros de la Asociación Libra y para ello necesitarán los 2/3 de votos a favor.

Esta Asociación es la única capaz de crear o destruir las criptomonedas. Pero para ello debe estar siempre vinculada con los activos de los fondos de reserva.

Así las monedas se crean cuando aquel autorizado por la Asociación le compra a esta una determinada cantidad de monedas por medio de activos fiduciarios capaces de respaldar esa nueva cantidad.

La operación contraria (venta de activos por un tercero a la Asociación) genera la destrucción de la moneda.

Así, como el valor de la moneda al momento de vender será igual al valor de la canasta establecido por la reserva, ello genera la estabilidad buscada por la moneda.

Resumiendo, podemos decir que Libra tiene como función crear un nuevo sistema financiero a través de una *blockchain* propia, respaldada por activos y controlada por una asociación independiente, cuyo objetivo es que cualquier persona pueda transmitir dinero como enviamos un mensaje de texto y poder incluir en el sistema financiero a aquellas personas que los bancos han rechazado en todos estos años.

Algo muy importante que debemos tener en cuenta a la hora de adquirir este activo es que, para poder hacer uso de Libra, debemos crear una *wallet* propia (hasta aquí como cualquier criptomoneda), pero con la característica que esa *wallet* solamente se podrá crear por medio de Calibra (empresa de Facebook) y para ello debemos brindar todos nuestros datos junto con una copia de nuestra identificación y una cuenta bancaria que la vincule (en caso de que la tengamos). Asimismo, le entregaremos a Calibra la posibilidad y libertad de utilizar nuestros datos.

Ante esto, Facebook ya ha dicho que respetará la privacidad de los usuarios, que no utilizará los datos para publicidad y que cumplirá con todas las normativas vigentes en cada país. Aquí solo nos queda creer en su palabra.

V. ¿Es Libra realmente una criptomoneda?

Si leemos detalladamente el White Paper, podemos observar grandes diferencias con la típica criptomoneda ya explicada.

Entre las principales diferencias encontramos primero la existencia de una Blockchain propia de un solo bloque. Esto nos hace cuestionarnos cuán grande será la confiabilidad y seguridad del sistema. Justamente la base del sistema Blockchain es su seguridad brindada por varios bloques interconectados de modo que si se afecta uno indirectamente se estará afectando a los subsiguientes, pero con una Blockchain de un solo bloque nos hace cuestionarnos como se puede evitar eso.

Otra de las diferencias con el resto de las criptomonedas es que aquellas no tienen un valor intrínseco y su fluctuación varía de acuerdo a las expectativas y al mercado. Mientras que Libra tiene un valor asignado por la Asociación Libra.

Y aquí tenemos la mayor diferencia de Libra. No es descentralizada, o al menos no lo pareciera.

Conforme su White Paper, se crea la Asociación Libra, justamente como núcleo del sistema que controle su funcionamiento y se mejore día a día. Ello va en contra de los principios establecidos originariamente en el Protocolo Bitcoin allá por el año 2008.

Si la intención de las criptomonedas era tener un sistema descentralizado, con la creación de la Asociación Libra ese tipo de sistema desaparecerá.

Incluso más, ésta Asociación, al establecer el valor intrínseco de la moneda, estaría haciendo las veces de un Banco Central. He aquí los grandes temores de los principales sistemas financieros del mundo y el porqué de que Libra tenga tantos enemigos.

Por el contrario, contiene todas las características de una criptomoneda al ser segura por su criptografía y la capacidad de transferir dinero a través de las fronteras de forma rápida e inmediata.

Ahora bien, más allá de la dicotomía entendemos que a los efectos jurídicos poco cambia. Se considere o no criptomoneda, su aplicación legal creemos que será igual.

No podrá ser considerada moneda porque no está regulada por el BCRA, y menos aún de curso legal en nuestro país.

Si bien su función es que sea un medio de pago, creemos que hasta que no alcance la masividad esperada no lo será, pero algo certero es que no podrá ser de tipo forzoso en nuestro país, ya que la única moneda aceptada es el peso.

Ahora bien, dependerá también de su lanzamiento final porque al encontrarnos con empresas como PayPal o Visa que forman parte de la Asociación Libra, quizás ellas por si misma generen la conversión de Libra a la moneda de curso legal de modo tal que el acreedor/receptor jamás se entere de que el deudor/pagador realizó el pago por medio de Libra.

Más allá de esto, al igual que cualquier otra criptomoneda (mas allá de las disquisiciones de si técnicamente lo es o no), entendemos que jurídicamente debiera considerarse a Libra una cosa virtual.

En base a esto nos viene la segunda pregunta, ¿es legal?

En nuestro país no hay ninguna norma que lo prohíba y, en base al art. 19 de nuestra constitución nacional, todo lo que no está prohibido está permitido, por lo tanto podemos concluir que sería legal su utilización.

De este modo *si las partes están de acuerdo se podrá intercambiar por otra cosa y hasta por dinero.*

VI. Implicancias Tributarias

La Ley de Impuesto a las Ganancias, estableció por medio de la Ley 27.430, la incorporación del término "moneda digital" a nuestro ordenamiento tributario.

Éste término se establece en paralelo al de "moneda virtual" ya expresado por la UIF al establecer que son 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.

Las mismas se diferencian del "dinero electrónico" por ser éste último un mecanismo para transferir digitalmente moneda fiduciarias, es decir monedas que tienen circulación legal (13).

Podemos decir entonces que "las monedas virtuales" se encuentran dentro del concepto de "moneda digital", incluso como expresamos en párrafos superiores, la gran mayoría de conceptos de criptomonedas se refieren a las mismas como "moneda digital".

Siguiendo la línea del Dr. Daniel Rybnik (14) cabe responder la pregunta sobre si la expresión "monedas digitales" prevista en la Ley de Impuesto a las Ganancias puede incluir a las "monedas virtuales", a la que cabe responder que ello únicamente podría ocurrir bajo el encuadramiento de su enajenación como resultado de fuente extranjera, y específicamente excluyendo la posibilidad de que califique como resultado de fuente argentina. De modo tal que el resultado por la cesión de "monedas virtuales" se encuentra alcanzado por el impuesto a las ganancias para personas humanas y sucesiones indivisas residentes en la Argentina a la alícuota del 15%, aún en el supuesto que no hagan de la enajenación su profesión habitual o comercio, y con independencia de cualquier otro factor (LIG, arts. 2, inc. 4º y 90, párr. 3º).

En cuanto al IVA, desde el momento en que las criptomonedas no pueden ser consideradas como "cosa", no se configura el elemento objetivo necesario para su tributación.

En lo referente a la Ley de Impuesto sobre los Bienes Personales, la misma contiene una exención expresa sobre los bienes inmateriales en su art. 21, inc. d), de modo tal que si consideramos a las criptomonedas como "cosa virtual" es decir como un bien inmaterial, se encuentra exenta del mismo.

Hasta aquí, todo lo expresado para la generalidad de las criptomonedas, y a pesar de las diferencias que Libra cursa con las mismas,

(13)"Prevención de Lavado de Activos (LA) y Financiación del Terrorismo (FT). Res. (UIF) 300/2014", Práctica Profesional, La Ley, nro. 220, agosto 2014.

(14) "Una aproximación a la tributación de las criptomonedas" – "Tributación de la Economía Digital" – Capítulo 18 – Ed. La Ley 2019.

igualmente sería aplicable a la materia en estudio en el presente.

Un punto importante al cual hacer referencia es en cuanto al impuesto a los débitos y créditos bancarios. Como quedó expresado en el presente artículo, la principal función de Libra será permitir el acceso a pagos electrónicos a aquellas personas que se encuentran fuera del sistema financiero bancario mundial. Su objetivo será convertirse en el medio de pago para operaciones a realizarse a través de Facebook (compras en el Market de la plataforma nombrada) o compras internacionales y/o nacionales que utilicen como sistema de pago PayPal, o incluso enviar dinero y/o pagos por medio de mensajería instantánea como es Whatsapp.

Sea cual sea el sistema de pago, lo cierto es que estaremos enviando un bien inmaterial, una cosa virtual, con lo cual no puede considerarse que la misma sea una transferencia de fondos, y por consiguiente tampoco encuadraría en este tributo.

VII. ¿Cómo puede afectar a un consumidor/usuario?

Como fue desarrollado en párrafos anteriores, el sentido de Libra es generar un nuevo medio de pago para aquellas personas que no están bancarizadas, de este modo podrán adquirir productos a través del Market Place de Facebook o pagar servicios a través de Visa o PayPal utilizando como medio de pago a Libra.

Ahora bien, la primera pregunta que nos viene a la mente es ¿Qué pasa si compro un producto utilizando como medio de pago a Libra y no recibo ese producto, o el mismo me vino fallado? ¿Puedo reclamar contra la Asociación Libra como parte de la cadena del consumidor? (15)

A mi entender para responder esa pregunta debiéramos estar al caso puntual. Pareciera (al menos así fue promocionado) que aquellos usuarios que utilicen Libra para comprar tendrán un descuento en el valor del producto o del servicio. Si éste es el caso, consideramos que perfectamente la Asociación Libra fue parte de la cadena comercial y por lo tanto solidariamente responsable.

Lo mismo pasará si indebidamente aquel miembro de la Asociación Libra (ej. PayPal) descontase indebidamente más dinero del que corresponde a la hora de hacer la conversión de Libra a la moneda Fiat.

Pero por desgracia no todo es color de rosa, porque en este punto es necesario recordar que la Asociación Libra no tiene sede en nuestro país, ni aún filial (quizás sí en un futuro pero no en el presente). Su sede está en Suiza, por lo tanto habría que analizar la practicidad de si realmente es recomendable demandar también a una empresa que tiene su sede en Suiza por haber sido la promotora del descuento.

En igual sentido nos preguntamos qué pasaría si habiendo adquirido x cantidad de moneda Libra en una promoción realizada por ejemplo por PayPal, se nos acreditan en nuestro wallet menor cantidad o los descuentos a la hora de comprar no se aplican. Acá nos genera las dudas acerca de si la Asociación Libra es un ente diferente de PayPal (a simple vista pareciera que así lo es) para demandar a todos en la cadena de consumo, pero nuevamente vamos a tener los conflictos de las sedes a la hora de demandar a los posibles resultados. Al día de hoy no podemos encontrar una solución práctica para esta posible hipótesis, habrá que esperar a que Libra salga al mercado para tomar nota de su modus operandi y ahí recién establecer un nuevo análisis de los actores implicados en su comercialización.

Cuestiones que también nos surgen y que al día de hoy tampoco tenemos respuesta, es si aparecerán casas de cambio o Exchange que permitan cambiar la moneda Fiat por Libra u otra criptomoneda por ésta. Porque en ese caso podrían generarse desde estafas al consumidor hasta abusos por los valores en las tasas de cambio. Pareciera que, por la función del sistema y la centralización de Libra en base a su Asociación, no tendrán permitido los Exchange hacer uso de esto pero ello hasta su lanzamiento no lo sabremos con certeza.

Por otro parte, desde el anuncio de su publicación, ya se han generado gran cantidad de es-

(15) Art. 13, Ley 24.240.

tafas referidas a supuestas casas de cambio que ofrecen la preventa de la moneda (16).

Y finalmente lo que más escozor nos genera es respecto a los datos personales. Como se expresó párrafos anteriores, como punto necesario para la creación del wallet Calibra, aquella persona que quiera acceder al sistema deberá brindar todos sus datos y cedérselos gratuitamente a esta empresa, que no es ni más ni menos que Facebook.

Recordemos que Facebook ya ha tenido más de una vez conflictos por el uso de los datos de sus usuarios, usos que han ido desde la publicidad hasta utilización con fines políticos.

Si bien, se comprometen a cumplir con toda la normativa de privacidad y utilización de datos de cada país, y manifiestan que el hecho de recabar los datos es solamente para evitar el lavado de dinero y terrorismo propio de la gran mayoría de las criptomonedas, vuelvo a repetir que con el antecedente de la empresa no es fácil creer que cumplirán con su palabra.

Creemos que como operadores del derecho debemos mantenernos objetivos en el tema y brindar la mayor cantidad posible de información a los potenciales consumidores de Libra, para ello sería recomendable que organizaciones de defensa del consumidor lleven adelante publicidad y sistemas de información respecto de las implicancias de este tipo de operaciones así como de los derechos y protección de los datos personales de cualquier usuario/consumidor de estos sistemas.

VIII. Conclusiones

En conclusión una vez más el gigante de las comunicaciones ha logrado revolucionar al mundo con solamente un aviso, y si bien Libra tiene una receta que incluye en la olla a grandes nombres del intercambio financiero como son MasterCard, Visa, EBay, MercadoPago y PayPal, empresas Fintech como Uber y Spotify, empresas de tecnología blockchain como Coinbase, Alastria y de la comunicación y marketing como es Facebook a través de su filial recién creada Calibra; habrá que ver si su masividad y su funcionamiento genera un buen sabor para el consumidor/usuario de estos sistemas.

Por otro lado, la masividad y marketing de Facebook en conjunto con el sistema centralizado que tiene Libra, puede llegar a poner en jaque a los sistemas bancarios como hoy los conocemos. Ello genera los miedos de los grandes bancos mundiales que ven en Libra un potencial competidor a gran escala y que solo el futuro demostrará si sus temores son o no fundados.

Pero, más allá de esto, creo que lo que hay que considerar es que lo más importante al momento de su despegue no será el valor de libra sino el valor de nuestros datos.

(16) *https://www.infobae.com/america/tecno/2019/07/23/libra-la-criptomoneda-de-facebook-ya-es-blanco-de-los-estafadores/.*

Consideraciones sobre la Resolución UIF 76/2019 para las tarjetas de pago

JUAN M. DIEHL MORENO (*) Y **SANTIAGO E. ERASO LOMAQUIZ** (**)

I. Introducción

Con la emisión de la Resolución 76/2019 (la "Resolución"), la Unidad de Información Financiera (UIF) ha actualizado notablemente el marco normativo sobre prevención del lavado de activos y financiación del terrorismo (LA/FT) aplicable al sector de los medios de pago. Específicamente, a la industria de las tarjetas de pago y cheques de viajero.

El desarrollo del mercado de los prestadores de servicios financieros no regulados por el Banco Central de la República Argentina (BCRA), junto con la finalidad del Estado de fomentar la inclusión financiera y la formalización de la economía, han impactado en la necesidad de actualizar el régimen anteriormente regulado por la Resolución UIF 2/2012.

Estos prestadores, a los cuales nos referiremos como Fintech, se caracterizan por desarrollar un modelo de negocios centrado en la utilización de las tecnologías de la información y la comunicación para el otorgamiento de servicios financieros. Su actividad y creciente relevancia en el mercado han llevado a las principales autoridades financieras a adecuar sus marcos regulatorios a las exigencias del mercado actual (1).

II. Novedades de la Resolución

La Resolución ha incorporado diversas modificaciones tendientes a adaptar el marco regulatorio a los cambios del mercado para que incluya nuevas categorías de sujetos obligados, definiciones, medidas de debida diligencia e, incluso, el enfoque del sistema de prevención de LA/FT.

A continuación, analizaremos someramente algunos de los principales cambios normativos introducidos por la Resolución, focalizándonos en su impacto sobre la industria de las tarjetas de pago operadas a través de modelos de negocios propios de las Fintech.

2.1. Enfoque basado en riesgo

2.1.1. Aspectos generales

Siguiendo con la reforma normativa iniciada con la Resolución UIF 30/2017 (2), la UIF ha in-

(*) Abogado por la Pontificia Universidad Católica Argentina. Máster en Derecho Empresario en la Universidad Austral. Máster en Leyes por la Universidad de Northwestern.

(**) Abogado por la Universidad Austral. Miembro de la Comisión de Derecho de la Alta Tecnología del Colegio de Abogados de la Ciudad de Buenos Aires.

(1) Tanto el Banco Central de la República Argentina, la Comisión Nacional de Valores, y la Unidad de Información Financiera han realizado esfuerzos notables para analizar el impacto de los nuevos modelos de negocios existentes y actualizar los marcos normativos de sus respectivas competencias.

(2) Aplicable a entidades financieras y cambiarias.

corporado el enfoque basado en riesgo (EBR) a los requisitos de prevención de LA/FT para los emisores y operadores de tarjetas de pago y cheques de viajero.

El EBR fue incorporado por el Grupo de Acción Financiera Internacional (GAFI) en la primera de las recomendaciones de sus "Estándares Internacionales sobre la Lucha contra el Lavado de Activos y el Financiamiento del Terrorismo y la Proliferación" (las "Recomendaciones") (3).

El principal objetivo del enfoque basado en riesgo es promover una mayor eficiencia y precisión en la asignación de esfuerzos y recursos para la prevención del LA/FT, asignando medidas reforzadas para aquellos casos en los que se identifiquen mayores riesgos, e implementando medidas simplificadas para aquellos en los que los riesgos identificados sean bajos. En suma, se intenta lograr una proporcionalidad entre el riesgo identificado y las medidas a adoptar.

La primera Recomendación del GAFI determina que los países deberán requerir a los sujetos obligados (4) que identifiquen, analicen y tomen acciones efectivas para mitigar sus riesgos de LA/FT. Este tipo de enfoque intenta armonizar el objetivo estatal de contar con un sistema normativo adecuado para la prevención de LA/FT, con la necesidad de los sujetos obligados de no ver restringida la innovación en sus modelos de negocios lícitos. El GAFI ha dicho que el EBR no debe ser diseñado para prohibir que los sujetos obligados lleven a cabo relaciones comerciales con sus clientes (actuales o potenciales), sino que debe asistir a dichos sujetos para gestionar de forma efectiva los potenciales riesgos de LA/FT (5).

En una industria como la Fintech, la existencia de regulaciones formalistas que impongan procedimientos que impliquen ralentizar o complejizar la experiencia del cliente pueden devenir en barreras infranqueables para operar en el mercado. Más aún, por ejemplo, en aquellos casos en los que las regulaciones impongan la necesidad de contar con la presencia física de los clientes para llevar a cabo determinados procedimientos, como sucede con la identificación presencial.

Cabe destacar que en un sistema basado en el EBR es probable que los sujetos obligados no adopten prácticas idénticas de prevención de LA/FT. En tal sentido, el propio GAFI ha explicado que la implementación del EBR requerirá que se les otorgue a los sujetos obligados la oportunidad de elaborar apreciaciones razonables.

Dicho organismo expresa que sin perjuicio de la fuerza y efectividad de los controles de prevención de LA/FT establecidos por un sujeto obligado, los criminales continuarán intentando mover fondos de origen ilícito a través del sector financiero sin ser detectados y, en ciertas ocasiones, tendrán éxito. No obstante ello, los reguladores y autoridades judiciales deben tener en cuenta y considerar adecuadamente los EBR bien razonados de los sujetos obligados. Cuando estos no mitiguen efectivamente los riesgos como resultado de una falta de implementación o diseño adecuada del EBR, el GAFI insta a los reguladores y autoridades judiciales a imponer las sanciones y remedios apropiados (6).

A tal efecto, los considerandos de la Resolución recuerdan que las Recomendaciones del GAFI establecen que los países deben exigirles a los sujetos obligados que cuenten con políticas, controles y procedimientos que les permitan gestionar y mitigar con eficacia los riesgos de LA/FT que se hayan identificado. Aclaran también que, desde un EBR, corresponde establecer para casos de inobservancia parcial o cumplimiento defectuoso de alguna de las obligaciones y deberes impuestos en la normativa la posibilidad que la UIF pueda disponer

(3) Emitidas el 16 de febrero de 2012 y actualizadas en forma periódica.

(4) Las Recomendaciones utilizan la terminología propia del GAFI, refiriéndose a entidades (instituciones) financieras y a "Actividades y Profesiones No Financieras Designadas", entre las cuales se encuentran los emisores y operadores de tarjetas de pago. Al respecto, el GAFI determina que los países deben analizar la forma en la que se implemente el EBR teniendo en cuenta la capacidad y experiencia sobre prevención de LA/FT de cada sector.

(5) Cfr. FATF-GAFI, *Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing*, junio, 2007.

(6) FATF-GAFI, *Guidance on the Risk-Based Approach*..., cit.

acciones correctivas idóneas y proporcionales, necesarias para subsanar los procedimientos o conductas observadas.

2.1.2. Factores de riesgo

Una de las notas destacables del EBR consiste en la enumeración, no taxativa, de cuatro factores de riesgo que los sujetos obligados deberán tener en cuenta para confeccionar su autoevaluación de riesgos y gestionar los riesgos identificados.

Siguiendo con las Recomendaciones, la UIF ha mantenido los mismos factores de riesgo principales que los utilizados para la Resolución UIF 30/2017. Estos son: (i) clientes, (ii) productos y/o servicios, (iii) canales de distribución, y (iv) zona geográfica.

Mientras que los clientes, los productos y/o servicios y las zonas geográficas fueron reconocidos generalmente como factores de riesgo de LA/FT (7), los canales de distribución cobraron una relevancia significativa desde la irrupción de las tecnologías de la información y la comunicación en la prestación de servicios financieros. Los riesgos asociados a los diferentes modelos de distribución (operatoria por Internet, operatoria telefónica, distribución a través de dispositivos móviles, operatividad remota, entre otros) (8) han devenido en una categoría autónoma a ser analizada por los sujetos obligados.

En adición a los factores enunciados por la Resolución, existen ciertos factores de riesgo específicos para las tarjetas y los nuevos medios de pago, tales como (i) los medios disponibles para el fondeo de las tarjetas, (ii) la posibilidad de obtener dinero en efectivo a través de las tarjetas, y (iii) la segmentación de los servicios (9).

Con respecto a la última categoría, destacamos que la participación de múltiples actores resulta común en la industria de las tarjetas de pago. Más aún, la propia UIF ha reconocido la relevancia de la segmentación del mercado al expresar en sus considerandos de la Resolución que, a diferencia de la Resolución UIF 2/2012, pone énfasis en las tareas vinculadas a la administración y operación de estos medios de pago. La UIF explica que "debido a un cambio en la composición del sector de tarjetas de crédito y compra, corresponde precisar el alcance del concepto de operador de tarjeta de crédito y compra adecuándolos a la realidad imperante en el mercado, y los roles que cumplen los Sujetos Obligados en cada caso [...] por ello, se incorporan los conceptos de 'Adquirente', 'Agregadores', 'Agrupadores' y 'Facilitadores de Pagos', por su carácter de Operadores de Tarjeta de Crédito y Compra".

2.2. Definiciones y sujetos obligados

2.2.1. Tarjeta de crédito

La Resolución define a la tarjeta de crédito utilizando la misma definición que la ley 25.065 de Tarjetas de Crédito (LTC) utiliza para definir al "sistema de tarjeta de crédito". De tal modo, el art. 2°, inc. y), de la Resolución define a la tarjeta de crédito como el "conjunto complejo y sistematizado de contratos individuales cuya finalidad es posibilitar al usuario efectuar operaciones de compra o locación de bienes o servicios u obras, enviar dinero, obtener préstamos y anticipos de dinero del sistema, en los comercios e instituciones adheridos; diferir para el titular responsable el pago o las devoluciones a fecha pactada o financiarlo conforme alguna de las modalidades establecidas en el contrato; o abonar a los proveedores de bienes y servicios los consumos del usuario en los términos pactados" (10).

Resulta sutil, aunque potencialmente relevante, el modo en el que la UIF ha enumerado las finalidades del sistema de tarjeta de crédito. En vez de seguir la forma utilizada por la LTC, la UIF ha escogido enumerarlas con puntos y comas, utilizando la conjunción coordinante "o" entre la segunda y la última, dando a entender que las finalidades podrían ser alternativas.

Del mismo modo, y a diferencia de la LTC, la Resolución no provee una definición de tar-

(7) Cfr. FATF-GAFI, *Guidance on the Risk-Based Approach*..., cit.

(8) Resolución UIF 76/2019, art. 5°, inc. c).

(9) FATF-GAFI, *Guidance for a Risk-Based Approach. Prepaid Cards, Mobile Payments and Internet-Based Payment Services*, junio, 2013.

(10) Cfr. Ley 25.065 de Tarjetas de Crédito, art. 1°.

jeta de crédito, en tanto instrumento. Mientras que la LTC aclara que "[s]e denomina genéricamente Tarjeta de Crédito al instrumento material de identificación del usuario, que puede ser magnético o de cualquier otra tecnología, emergente de una relación contractual previa entre el titular y el emisor" (11), la Resolución guarda silencio en cuanto a los soportes e instrumentos utilizados para operar el sistema de las tarjetas.

Sin perjuicio de ello, como veremos *infra*, entendemos que una interpretación armónica del sistema jurídico debería permitir interpretar que la denominación "tarjeta" corresponde al instrumento material de identificación del usuario, como lo define la LTC, sea para el caso de las tarjetas de crédito, débito (no comprendidas por la Resolución), compra o prepagas.

2.2.2. Tarjeta de compra

La Resolución también ha seguido a la LTC a la hora de definir a las tarjetas de compra. No obstante, en este caso la UIF también ha optado por incluir algunas diferencias con el texto de la LTC.

El art. 2°, inc. z), de la Resolución define a la tarjeta de compra como "[a]quella que las instituciones comerciales entregan a sus clientes para realizar compras en establecimientos comerciales". A diferencia de la LTC, la UIF ha decidido no incluir la palabra "exclusivas" luego de "compras", y tampoco distingue entre establecimientos y sucursales.

Entendemos que la interpretación de ambas definiciones debe ser, no obstante, sustancialmente similar. La definición de la Resolución parece ser más llana y libre de términos que —como la palabra "exclusivas"— resultan innecesarios para comprender que se trata de un instrumento material de identificación del usuario que las instituciones comerciales otorgan a sus clientes, y cuya única finalidad debe ser permitirles efectuar compras en sus establecimientos.

2.2.3. Tarjeta prepaga

La Resolución utiliza un concepto de tarjeta prepaga distinto de aquel contenido en la Resolución UIF 2/2012, la cual se refería a las tarjetas que, sean recargables o no, funcionen contra saldos que son acreditados previamente a su uso y sean destinados a la compra de un bien o servicio (12).

Al igual que la anterior, la nueva normativa no define específicamente a las tarjetas prepagas, sino que presenta el concepto bajo el cual debe entenderse encuadrada la actividad de los "operadores de tarjetas prepagas" al momento de establecer su carácter de sujeto obligado. La Resolución se refiere a las tarjetas prepagas, recargables o no, que operan contra saldos acreditados previamente a su uso y sean destinados a la compra de bienes o servicios en establecimientos comerciales. Esta norma también agrega que se encuentran incluidas dentro de su ámbito de aplicación las "tarjetas prepagas de regalo", sin definirlas.

No estamos de acuerdo con la limitación teleológica del concepto de tarjeta prepaga a su utilización para la compra de un bien o servicio. La evolución que han experimentado las tarjetas prepagas desde su creación ha avanzado hasta convertirlas —en muchos casos junto con prestaciones adicionales— en herramientas que exceden por mucho el mero intercambio comercial (13). En efecto, las tarjetas prepagas se han transformado en una herramienta de acceso a los fondos acreditados en las cuentas contra las cuales giran, los cuales pueden ser asignados para intercambios comerciales, transferencias, donaciones, inversiones, solicitud de préstamos, entre otras actividades. A los efectos del presente trabajo, nos referiremos a estos fondos acreditados para el uso de las tarjetas prepagas como las "cuentas".

Téngase como prueba de la relevancia de este tipo de instrumentos, y de cómo su utilización excede el mero intercambio comercial, la creación por el BCRA de la Clave Virtual Uniforme

(11) Ley 25.065 de Tarjetas de Crédito, art. 4°.

(12) Resolución UIF 2/2012, art. 2°, inc. a).

(13) El cual, por cierto, no se limita a la "compra" de bienes y servicios.

(CVU) (14), dirigida a facilitar la interoperabilidad entre los clientes de los proveedores de servicios de pago —muchos de ellos, Fintech— y otros clientes de las entidades financieras.

Por lo tanto, entendemos que no podemos hablar de la relevancia de las tarjetas prepagas sin hablar de la relevancia de las cuentas asociadas a las mismas. Analizaremos *infra* algunas derivaciones de este punto. Sin perjuicio de ello, en esta sección nos enfocaremos en esclarecer el concepto de tarjeta prepaga —en tanto instrumento de pago— y sus modalidades bajo la Resolución.

2.2.3.1. Recargables y no recargables

Las tarjetas prepagas serán recargables cuando admitan nuevos ingresos de fondos a las cuentas contra las cuales giran, mientras que no serán recargables cuando no permitan esta opción.

El ingreso de fondos a las tarjetas recargables puede llevarse a cabo a través de distintas modalidades, entre ellas, mediante transferencias bancarias, transferencias desde otras tarjetas prepagas, y la entrega de dinero en efectivo.

Al respecto, siguiendo con lo analizado en otros trabajos (15), entendemos que existe una estrecha relación entre la entrega de dinero por parte de los clientes y el contrato de depósito irregular del art. 1367 del Cód. Civ. y Com. No obstante, el contrato de depósito no acaba por definir la naturaleza de la relación jurídica entre el cliente y el prestador de servicios de pago. Considerando que la finalidad de custodia que caracteriza al depósito no constituye el objeto principal de la relación con el prestador de servicios de pago, no creemos que esta figura resulte adecuada para definir acabadamente su naturaleza.

Sostenemos que, desde una perspectiva global, el contrato de emisión de tarjeta prepaga constituye un contrato innominado, enmarcado en un grupo de contratos conexos que conforman el sistema de tarjetas prepagas, dirigido a la prestación de un servicio de pagos, caracterizado, principalmente (16), por la emisión de instrumentos para ser utilizados por los clientes como forma de cancelación de obligaciones con comercios adheridos (17).

En tanto contratos innominados, deben encontrarse regidos —en primer lugar— por las disposiciones de orden público aplicables, y —en segundo lugar— por los elementos establecidos en el art. 970 del Cód. Civ. y Com. en el siguiente orden de prelación: (i) la voluntad de las partes, (ii) las normas generales sobre contratos y obligaciones, (iii) los usos y prácticas del lugar de celebración, y (iv) las disposiciones correspondientes a los contratos nominados afines que son compatibles y se adecúan a su finalidad (18).

2.2.3.2. Circuito cerrado

Se conoce como tarjetas prepagas de circuito cerrado a aquellas que permiten ser utilizadas en un entorno limitado, pudiendo ser aceptadas únicamente por un número determinado de comercios adheridos. Un caso usual de este tipo de tarjetas prepagas son las denominadas tarjetas prepagas de "regalo".

No obstante, no debe entenderse que existe una identidad entre el concepto de tarjetas prepagas de circuito cerrado y las tarjetas de "regalo". Estas últimas son usualmente emitidas "al portador" con un valor monetario asociado a la tarjeta, la cual usualmente no es recargable.

Las tarjetas de circuito que no son de regalo pueden consistir en tarjetas prepagas, recargables o no, que se utilicen solamente dentro de un entorno limitado. Por ejemplo, este tipo de tarjetas son útiles para que los transportistas puedan utilizarlas en comercios determinados que se encuentren dentro de su itinerario. La tarjeta no podría ser utilizada en otros comercios que no sean aquellos designados previa-

(14) Cfr. BCRA, Comunicación "A" 6510 y ccds.

(15) Eraso Lomaquiz, Santiago E., *El dinero electrónico en el Derecho Argentino (Conclusión)*, La Ley, 3/1/2017, LL-2017-A.

(16) Aunque no limitado a ello.

(17) Para un análisis sobre las diferencias entre los contratos de mutuo, depósito irregular y bancario con relación al dinero electrónico, ver Eraso Lomaquiz, Santiago E., *El dinero electrónico…*, cit.

(18) Cfr. Eraso Lomaquiz, Santiago E., cit.

mente, pero podría ser recargada y podría ser emitida a nombre de una persona determinada.

2.2.3.3. Circuito abierto

Las tarjetas prepagas de circuito abierto, recargables o no, son aquellas que permiten ser utilizadas dentro de un grupo extenso de comercios adheridos a una red de tarjetas (19).

La mayor parte de las tarjetas prepagas de circuito abierto giran contra una cuenta existente con un prestador de servicios de pago. Adicionalmente, este tipo de tarjetas (y sus cuentas asociadas) suelen permitir una amplia gama de operaciones, incluyendo transferencias de fondos, pago de bienes y servicios, y retiro de dinero a través de redes de cajeros automáticos.

Este tipo de tarjetas prepagas son mayormente comercializadas por Fintech, y son consideradas como una herramienta de inclusión financiera y formalización de la economía. Sin perjuicio de ello, teniendo en cuenta el amplio rango de operaciones que permiten, son consideradas como un medio idóneo para la comisión de LA/FT (20).

2.2.4. Sujetos obligados

2.2.4.1. Operadores de tarjetas de crédito, compra o prepaga

De acuerdo con el inc. w) del art. 2° de la Resolución, son considerados como sujetos obligados las empresas emisoras de cheques de viajero y las entidades que actúan como operadores del sistema de tarjetas de crédito o compra. La misma norma indica que por operadores del sistema de tarjetas de crédito o compra se debe entender incluyendo a los emisores de tarjeta de crédito o compra, así como también a los adquirentes, agregadores, agrupadores y facilitadores de pagos.

La norma aclara que también se considerarán comprendidos como sujetos obligados a los operadores de tarjetas prepagas, incluidas las tarjetas prepagas de regalo, recargables o no, que operan contra saldos acreditados previamente a su uso y sean destinados a la compra de bienes o servicios en establecimientos comerciales (21).

Entendemos que, al referirse a operadores de tarjetas prepagas, la norma intenta remitir al concepto de operadores del sistema de tarjetas de crédito o compra. Por lo tanto, consideramos que la Resolución comprende como sujetos obligados a los emisores de tarjetas prepagas, así como también a los adquirentes, agregadores, agrupadores y facilitadores de pagos en el sistema de tarjetas prepagas.

Los considerandos de la Resolución aclaran los motivos de la extensión del concepto de sujetos obligados respecto de la anterior Resolución UIF 2/2012. Expresa que dicha modificación responde al "cambio en la composición del sector de tarjetas de crédito y compra", por lo cual "corresponde precisar el alcance del concepto de operador de tarjeta de crédito y compra adecuándolos a la realidad imperante en el mercado, y los roles que cumplen los Sujetos Obligados en cada caso". Por lo tanto, la norma incorpora los conceptos de "Adquirente", "Agregadores", "Agrupadores" y "Facilitadores de Pagos", por su carácter de Operadores de Tarjeta de Crédito y Compra (22).

Destacamos que dicha extensión podría resultar de una interpretación del concepto de emisor de tarjetas de crédito de la LTC, en tanto la misma los identifica como aquellas entidades financieras, comerciales o bancarias que emitan las tarjetas de crédito, o *que hagan efectivo el pago*. El alcance del concepto de "hacer efectivo el pago" es susceptible de diferentes interpretaciones, entre las cuales puede incluirse la de encuadrar a los adquirentes, agregadores, agrupadores y facilitadores de pagos.

(19) Entre ellas, Visa y MasterCard.

(20) FATF-GAFI, *Guidance for a Risk-Based Approach. Prepaid Cards...*, cit. Destacamos que las tarjetas prepagas de circuito cerrado, recargables o no, también poseen potencialidad para ser utilizadas para la comisión de LA/FT, aunque el riesgo asociado a aquellas resulte menor.

(21) Ver *supra* nuestro análisis sobre las tarjetas prepagas.

(22) Agregamos que, como fue indicado *supra*, el concepto de operadores no debe limitarse a las tarjetas de crédito y compra.

2.2.4.2. Adquirentes, Agregadores, Agrupadores y Facilitadores de Pagos

A los efectos de la Resolución, se entiende por "adquirente" a aquella persona humana, jurídica o estructura legal sin personería jurídica que realice algunas de las siguientes tareas vinculadas con la operación de tarjetas de pago: (i) adherir a comercios al sistema de tarjetas de crédito, o (ii) liquidar al receptor de pagos el importe de los pagos con tarjetas que cuenten con la autorización de pago otorgada por el correspondiente emisor.

La Resolución encuadra a los agregadores, agrupadores y facilitadores de pagos dentro de un mismo concepto, refiriéndose a ellos en grupo en toda ocasión. La norma define el rol de agregador, agrupador o facilitador de pagos como aquel que desempeña una persona humana, jurídica o estructura legal sin personería jurídica, que mediante un contrato con el adquirente, proporciona a sus clientes, a través de una plataforma o sistema, el servicio de procesamiento y/o liquidación de pagos de las tarjetas a través de diversos medios, ya sea en contexto de medios de pago presencial como no presencial (23).

Al contemplar la actuación de estos participantes del mercado, la Resolución se ha adelantado a la LTC, cuyo texto no termina de reflejar aspectos importantes de la realidad actual. Son varios los proyectos que se han presentado en el Congreso de la Nación para adecuar a la LTC al mercado actual, aunque no han logrado convertirse en ley (24).

2.2.5. Sujetos excluidos

La Resolución excluye expresamente su aplicación a (i) los operadores de la tarjeta que instrumenta el Sistema Único de Boleto Electrónico (SUBE), (ii) los operadores de tarjetas destinadas exclusivamente a la adquisición de bienes consumibles dentro del local comercial emisor de la tarjeta, y (iii) los operadores de tarjetas destinadas exclusivamente a la carga de combustibles y lubricantes. Atento a que la Resolución UIF 2/2012 ya incluía la excepción para la tarjeta SUBE (25), nos enfocaremos en los dos supuestos restantes.

La segunda excepción cuenta con tres elementos principales. En primer lugar, en cuanto a las personas comprendidas, abarca a los operadores de tarjetas, pero sólo respecto de su actividad relacionada a las tarjetas emitidas por quien explota los locales comerciales dentro de los cuales deben consumirse los bienes adquiridos.

El segundo elemento versa sobre la finalidad de las tarjetas. Esta finalidad debe cumplir con dos requisitos, uno relacionado con los bienes que se puedan adquirir con la tarjeta, mientras que el otro se centra en la ubicación en la cual estos bienes deben ser consumidos. Los bienes deben ser consumibles y deben encontrarse destinados a ser consumidos en el local comercial del emisor de la tarjeta.

Con respecto a los bienes consumibles, entendemos que la Resolución se refiere al concepto que el art. 231 del Cód. Civ. y Com. esboza respecto de las cosas consumibles. Este artículo las define como "aquellas cuya existencia termina con el primer uso", contrastando con las cosas no consumibles, que son "las que no dejan de existir por el primer uso que de ellas se hace, aunque sean susceptibles de consumirse o deteriorarse después de algún tiempo".

Al utilizar la expresión bienes, y no cosas, resulta menos claro el límite del alcance de la excepción. Por un lado, podría entenderse que aquellos bienes inmateriales que resulten "consumibles" por dejar de existir por el primer uso quedarían incluidos dentro de este supuesto. Tal sería el caso de una tarjeta prepaga emitida por un complejo de cines para que sus beneficiarios puedan adquirir entradas para las distintas funciones. El derecho a ingresar a la sala de cine y ver la función —el bien adquirido— quedará extinto con el primer uso. Lo mismo sucedería con entradas para recitales, eventos

(23) Resolución UIF 76/2019, art. 2°, inc. c).

(24) Al respecto, ver el dictamen de la Comisión de Industria y Comercio de la Honorable Cámara de Senadores de la Nación, Orden del Día N° 277, impreso el 31/5/2017.

(25) Resolución UIF 42/2012.

deportivos, ciertos bienes digitales en entornos de videojuegos, etcétera (26).

Por otro lado, también sería posible argumentar que las excepciones deben interpretarse en forma restrictiva. Bajo este prisma, la excepción debería limitarse a las cosas consumibles del art. 231 del Cód. Civ. y Com. siempre que, además, sean consumidas dentro del local comercial emisor de la tarjeta.

El tercer elemento consiste en el objeto sobre el cual recae la excepción, es decir, el tipo de tarjeta. La excepción no aclara si la tarjeta debe ser recargable o no, por lo que entendemos que ambas modalidades se encuentran abarcadas. Adicionalmente, las tarjetas deben haber sido emitidas por quien explote los locales comerciales en los cuales se consumen los bienes adquiridos. Por lo tanto, entendemos que no resultarían abarcadas aquellas tarjetas emitidas por personas que no exploten los locales comerciales, aunque se encuentren destinadas exclusivamente a la adquisición de bienes para ser consumidos dentro de estos.

Con respecto a la última excepción, entendemos que su alcance resulta claro, siendo aplicable a los emisores, adquirentes, agregadores, agrupadores y facilitadores de pagos de tarjetas prepagas limitadas a pagos para la carga de combustibles y lubricantes. En este caso, no encontramos limitaciones respecto a la persona del emisor de las tarjetas.

2.2.6. Clientes

Siguiendo con la línea de la Resolución UIF 2/2012, el art. 2°, inc. d), de la Resolución comienza su definición del concepto de cliente como "toda persona humana, jurídica o estructura legal sin personería jurídica, con la que se establece, de manera ocasional o permanente, una relación contractual de carácter financiero, económico o comercial", continuando con un listado de supuestos específicos.

A diferencia de la Resolución UIF 2/2012, la Resolución no hace referencia a las definiciones de la LTC, así como tampoco distingue entre clientes habituales y ocasionales. La norma define a los clientes en función del sujeto obligado con el que interactúen.

En particular, se consideran clientes del emisor de las tarjetas a los usuarios titulares, mientras que los comercios adheridos serán considerados clientes de los adquirentes, así como también de los agregadores, agrupadores o facilitadores, si estos existieren en el esquema de pago. La Resolución aclara que los titulares de las tarjetas no son considerados clientes de los adquirentes, agregadores, agrupadores y facilitadores de pagos.

2.2.7. Comercio adherido

Con acertado criterio, la Resolución tampoco ha remitido a la LTC para definir a los comercios adheridos. En la norma bajo análisis, estos son definidos como "aquellas personas humanas o jurídicas o estructuras legales sin personería jurídica que, en forma ocasional o habitual y por medio de un contrato celebrado con el Emisor, el Adquirente, o el Agregador, Agrupador o Facilitador de Pagos, proporcionan bienes, obras, o servicios al usuario de tarjetas aceptando percibir su pago en las condiciones establecidas en el mencionado contrato".

De este modo, se han incorporado los conceptos de adquirente, agregador, agrupador y facilitador de pagos. La Resolución tampoco hace referencia al sistema de tarjeta de crédito, en la definición de comercio adherido, la cual se encuentra presente en la LTC cuando delimita el concepto a aquel que "en virtud del contrato celebrado con el emisor, proporciona bienes, obras o servicios al usuario aceptando percibir el importe mediante el sistema de Tarjeta de Crédito" (27). Más aún, la Resolución no provee una definición de "sistema de tarjeta de crédito" y tampoco remite al concepto de la LTC. Entendemos que una correcta interpretación de la Resolución obliga a utilizar la definición provista por la LTC (28).

(26) Destacamos que en estos casos también sería necesario considerar el riesgo asociado a la reventa de estos bienes.

(27) Ley 25.065 de Tarjetas de Crédito, art. 2°, inc. f).

(28) El art. 1° de la LTC determina que "[s]e entiende por sistema de Tarjeta de Crédito al conjunto complejo y sistematizado de contratos individuales cuya finalidad es: a) Posibilitar al usuario efectuar operaciones

2.3. Identificación no presencial de clientes

Cabe recordar que el problema de la identificación de las personas en la interacción no presencial ha sido desde siempre uno de los principales obstáculos para la vinculación jurídica, especialmente en Internet.

Entre las modificaciones más relevantes respecto del régimen de la Resolución UIF 2/2012, la UIF ha mantenido la línea adoptada para los sujetos obligados del mercado de capitales, del sector asegurador, así como también para las entidades financieras y cambiarias al permitir efectuar la aceptación e identificación de clientes en forma no presencial.

La Resolución ha tomado una aproximación distinta de la utilizada para la normativa aplicable a los sectores referenciados. Mientras que la normativa aplicable al sector asegurador determina un marco general para la aceptación e identificación de clientes, las resoluciones aplicables tanto a las entidades financieras como al sector del mercado de capitales establecen un esquema alternativo entre dos modalidades principales para lo que se conoce como el "onboarding digital" (29).

Por su parte, la norma bajo análisis se enfoca en la utilización de técnicas biométricas, las cuales deben ser rigurosas, almacenables, auditables y no manipulables. Estos medios tecnológicos de identificación de clientes se encuentran dirigidos a "sustituir" la presencia física de las personas. Desde una perspectiva comparativa, la Resolución parece incluir estándares menos flexibles que aquellos aplicables a las entidades financieras, al sector del mercado de capitales y a la industria aseguradora.

El mismo art. 26 de la Resolución, determina que los sujetos obligados deben "realizar el análisis de riesgo del procedimiento de identificación no presencial a implementar, el cual deberá ser gestionado por personal debidamente capacitado a tales efectos". Entendemos que ello no significa que los sujetos obligados puedan utilizar cualquier tipo de procedimiento de *onboarding* digital, sino que la libertad de elección se encuentra limitada a aquellos medios electrónicos que cumplan con los requisitos determinados al principio del artículo, esto es con uso de técnicas biométricas rigurosas, almacenables, auditables y no manipulables. La implementación de estos procedimientos no se encuentra sujeta a la autorización previa por parte de la UIF (30).

De acuerdo con la Resolución, los medios electrónicos utilizados para la identificación no presencial de clientes deben contar con mecanismos de protección frente a fraudes por ataques tanto físicos como digitales. Este requisito destaca la relevancia de la ciberseguridad para la prestación de servicios financieros. Ante la falta de un plexo normativo como el emitido por el BCRA para las entidades financieras, entendemos que los mecanismos de protección deberán responder a aquellos estándares mínimos usualmente aplicables a cada industria, teniendo en cuenta las particularidades del mercado en el que opere cada sujeto obligado y el nivel de sofisticación que le resulte exigible por los niveles de riesgo de LA/FT a los que se encuentre expuesto (31).

Estos medios electrónicos deben ser empleados a efectos de verificar la autenticidad de la información proporcionada por los clientes, así como también los documentos o muestras biométricas recabadas. Al exigir que las "muestras biométricas del Cliente deberán ser obtenidas de un ser humano genuino que se encuentre presente al momento de la identificación", en-

---

de compra o locación de bienes o servicios u obras, obtener préstamos y anticipos de dinero del sistema, en los comercios e instituciones adheridos. b) Diferir para el titular responsable el pago o las devoluciones a fecha pactada o financiarlo conforme alguna de las modalidades establecidas en el contrato. c) Abonar a los proveedores de bienes o servicios los consumos del usuario en los términos pactados".

(29) Cfr. Resolución UIF 30/2017, art. 26, incs. a) y b).

(30) Ello sin perjuicio de que la UIF audite el cumplimiento de la Resolución con relación a dichos procedimientos. Adicionalmente, el análisis sobre la adecuación y eficacia operativa del procedimiento de identificación no presencial implementado deben ser incluidos expresamente en el informe del revisor externo independiente al que se refiere el inc. a) del art. 19 de la Resolución.

(31) Destacamos que en este tipo de mercados es común encontrar normas de autorregulación en materia de ciberseguridad, aunque en la mayor parte de los casos se encuentran principalmente dirigidas a la operación de los servicios.

tendemos que la UIF requiere que estas herramientas tecnológicas cuenten con las medidas necesarias que permitan acreditar que quien se encuentra proporcionando los datos biométricos sea efectivamente una persona humana. Por encontrarse "presente", cabe entender que la Resolución se refiere a la presencia física de la persona frente al dispositivo que extrae sus datos biométricos. Asimismo, la norma destaca que todo ello deberá ocurrir al momento de la identificación, por lo que no cabría dar por cumplido este requisito con la remisión de un paquete de datos biométricos extraídos previamente al momento de la identificación.

Adicionalmente a la identificación no presencial, los sujetos obligados deben verificar la autenticidad de la información o la documentación que proporcionen los clientes. Dicha información puede ser provista por medios electrónicos. Asimismo, la Resolución autoriza a los sujetos obligados a implementar medios automatizados para la verificación de la información. Para ello, los sujetos obligados deberán encontrarse en condiciones de evidenciar que el desempeño de estos mecanismos en la confirmación de la correspondencia y la inalterabilidad sean iguales o superiores a los de un agente humano.

No es necesario que la verificación de la documentación sea llevada a cabo al momento de la identificación, siempre que ocurra con anterioridad a que el cliente comience a utilizar los productos y servicios abarcados por la Resolución.

Finalmente, la norma establece un requisito de seguridad con relación al proceso de identificación y verificación de la documentación. Específicamente, la norma expresa que los procedimientos de análisis de la información, los documentos, las comparaciones de las muestras biométricas y las determinaciones de la presencia genuina del cliente deben ser efectuados lejos del dispositivo del cliente, en un lugar que no sea accesible para el mismo.

Entendemos que la "lejanía" a la cual se refiere el art. 17 de la Resolución se encuentra dirigida a que los sujetos obligados eviten efectuar dichos procedimientos en un entorno accesible al cliente o sus dispositivos. Entre otras razones, esta medida se justifica en la necesidad de evitar potenciales manipulaciones en procesos de vital relevancia para la identificación de los clientes (32).

2.4. Digitalización de procesos

La operatoria de las Fintech tiene a la digitalización de los procesos como uno de sus elementos caracterizadores. En este sentido, la mayoría de las transacciones, la documentación y la información recolectada y generada en el marco del giro comercial habitual de este tipo de empresas se encuentra contenida en soporte electrónico.

Resultaría incoherente que —atento al avance de los medios tecnológicos disponibles— una normativa dirigida a regular los aspectos de prevención de LA/FT exija la conservación de documentos e información en soporte físico a un tipo de industria centrada en la oferta de productos y servicios digitales. Más aún en un contexto en el que, como es el caso de las Fintech, se encuentran involucradas finalidades como la inclusión financiera y la formalización de la economía.

De este modo, la UIF ha regulado el deber de conservación de la documentación contemplando la operatoria digital, utilizando una redacción tecnológicamente neutra que consideramos atinada. Específicamente, la Resolución requiere a los sujetos obligados conservar la documentación listada en el art. 17 en "medios magnéticos, electrónicos u otra tecnología similar, protegidos especialmente contra accesos no autorizados". Esta norma elabora una enunciación abierta de medios tecnológicos para la conservación de la documentación e información, limitada únicamente por su seguridad contra accesos no autorizados.

2.5. Debida diligencia

Siguiendo el EBR, la Resolución establece un marco dentro del cual los sujetos obligados deben identificar, evaluar y gestionar los riesgos de LA/FT asociados a su operatoria. Para ello,

(32) Manipulaciones que podrían ser efectuadas por los propios clientes o por terceros que tomen ventaja de las vulnerabilidades de sus dispositivos.

los sujetos obligados deben tomar en consideración —como mínimo— los factores de riesgo enunciados por la Resolución y efectuar una autoevaluación de riesgos sobre cada una de las líneas de negocio sujetas a la regulación bajo análisis. Esta evaluación interna debe contemplar la suficiencia de los recursos asignados para mitigar los riesgos de LA/FT.

La Resolución determina tres niveles de riesgo de LA/FT, a los cuales corresponden tres niveles distintos de debida diligencia. La calificación del riesgo de cada cliente debe ser actualizada acorde con las políticas y procedimientos establecidos por cada sujeto obligado, y dentro de los plazos establecidos en el art. 30 (33).

Destacamos que la norma aclara que la ausencia o imposibilidad del cumplimiento con los deberes de identificación de clientes resultará un impedimento para el inicio de las relaciones comerciales sujetas a su aplicación. Asimismo, para el caso de relaciones comerciales preexistentes, los sujetos obligados que se encuentren imposibilitados de cumplir con estos requisitos deberán cesar en su continuación. Entendemos que tal requisito resulta razonable, toda vez que la identificación del cliente consiste en el primer paso lógico para llevar a cabo un adecuado análisis del riesgo de LA/FT.

Sin perjuicio de ello, el art. 31 de la Resolución determina la posibilidad de identificar a los clientes que resulten beneficiarios de tarjetas prepagas de regalo de ciclo cerrado al momento del empleo de estas. En estos casos, la Resolución les exige a los sujetos obligados a establecer controles y alertas a fin de detectar desvíos en la operatoria, considerando entre otros aspectos los montos operados, la frecuencia y modalidad de las operaciones, su recurrencia, los bienes involucrados, la coincidencia de beneficiario final, u otros parámetros que a juicio del oficial de cumplimiento permitan gestionar de forma adecuada el riesgo de LA/FT.

Adicionalmente, la Resolución permite que los sujetos obligados que no puedan cumplir con los requisitos de debida diligencia del cliente lleven a cabo un análisis de riesgo para evaluar la continuidad o no de la relación con estos (34). Esta disposición resulta especialmente útil en atención a la diversidad de contextos y operaciones en los que pueden operar los sujetos obligados bajo la Resolución, evitando un excesivo rigor formalista.

Sin perjuicio del nivel de riesgo asignado a cada cliente, la Resolución exige que todos los clientes sean objeto de seguimiento continuado con la finalidad de identificar, sin retrasos, la necesidad de modificación de su perfil transaccional y de su nivel de riesgo asociado.

III. El dinero electrónico

Sin perjuicio de los distintos avances normativos contenidos en la Resolución, debemos observar que todavía subsiste el vacío regulatorio respecto de los emisores de dinero electrónico.

Al respecto, destacamos que en el derecho argentino existe una norma que proporciona una primera aproximación conceptual al significado del dinero electrónico. Se trata de la Resolución UIF 300/2014 (35) que, luego de definir el concepto de monedas virtuales, las diferencia del dinero electrónico, al cual describe como "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" (36). Es preciso destacar que tal descripción no se encuentra dirigida a establecer una definición normativa del concepto de dinero electrónico, sino a presentar una aproximación funcional a los meros efectos de dife-

(33) De acuerdo con esta norma, la información y documentación de los clientes debe mantenerse actualizada con una periodicidad proporcional al nivel de riesgo. Sin perjuicio de ello, en ningún caso se podrá dejar de actualizar los legajos de clientes de riesgo bajo por un período mayor a los cinco años. Para aquellos clientes a los que se hubiera asignado un nivel de riesgo alto, la periodicidad de actualización de legajos no podrá ser superior a un año, y para aquellos de riesgo medio, a los dos años.

(34) Resolución UIF 76/2019, art. 21.

(35) Esta norma incorpora al marco regulatorio sobre la prevención del lavado de activos y financiación del terrorismo una serie de obligaciones especiales para los casos en los que los sujetos obligados tomen conocimiento o participen de operaciones en las que se utilicen monedas virtuales.

(36) Resolución UIF 300/2014, art. 2°, segundo párrafo.

renciarlo del objeto de su regulación, esto es, las monedas virtuales (37).

En la actualidad, siguiendo a la mayor parte de las legislaciones europeas y latinoamericanas, consideramos que es posible definir al dinero electrónico como aquel medio de pago consistente en la representación de un valor monetario exigible a su emisor, emitido contra el previo recibo de fondos (38), susceptible de ser almacenado en diversos soportes, y que se encuentra dirigido a ser aceptado por personas distintas del emisor del dinero electrónico.

Al respecto, resulta discutible la posibilidad de extender la aplicación de la citada regulación a aquellos instrumentos de dinero electrónico que no cuenten con un soporte físico. En efecto, como fuera explicado *supra*, una interpretación analógica respecto de lo establecido en la LTC nos revela que aquellas podrían ser definidas como un instrumento material de identificación del usuario, el cual puede ser magnético o de cualquier otra tecnología (39).

(37) Cfr. Eraso Lomaquiz, Santiago E., *El dinero electrónico en el Derecho Argentino*, La Ley, 2/1/2017, LL-2017-A.

(38) Lo cual subsume a este tipo de medios de pago dentro de la categoría de los sistemas de prepago. Cfr. Eraso Lomaquiz, Santiago E., cit.

(39) Cfr. Ley de Tarjetas de Crédito, art. 4°.

IV. Conclusiones

Consideramos que la Resolución implica un paso acertado en cuanto incorpora el EBR a la operatoria de las tarjetas de pago, al tiempo que les permite a los sujetos obligados digitalizar sus procesos.

Siguiendo con lo expresado *supra*, también entendemos que la UIF ha tomado una decisión acertada al no remitir a las definiciones de la LTC, cuyo texto no termina de reflejar la evolución del mercado de las tarjetas de pago. Este cambio de aproximación prueba la necesidad de adecuar el texto de la citada ley para recoger las particularidades de dicho mercado, cuidando de no establecer limitaciones innecesarias a la innovación.

No obstante, quedan aún varios aspectos de la prestación de servicios de pago que no cuentan con una regulación particular. Entre ellos, el dinero electrónico sin soporte material parecería quedar excluido del ámbito de aplicación de la Resolución, siendo difícil asociarlo al concepto de sujeto obligado bajo la misma, es decir: operadores de "tarjetas" de crédito, compra y prepagas, o emisores de cheques de viajero.

SE TERMINÓ DE IMPRIMIR EN LA 2DA. QUINCENA DE OCTUBRE DE 2019
EN LOS TALLERES GRÁFICOS DE "LA LEY" S.A.E. e I. - BERNARDINO RIVADAVIA 130
AVELLANEDA - PROVINCIA DE BUENOS AIRES - REPÚBLICA ARGENTINA