RDYNT
Número 2

Revista Derecho y Nuevas Tecnologías

Director: Pablo A. Palazzi

DOCTRINA

CeTyS
Universidad de San Andrés

RDYNT

Número 2

Revista Derecho y Nuevas Tecnologías

RDYNT - Revista Derecho y Nuevas Tecnologías N.º 2, 2020
CDYT - COLECCIÓN DERECHO Y TECNOLOGÍA

RDYNT - Revista Derecho y Nuevas Tecnologías
ISSN 1514-1918
Buenos Aires, Argentina.

Diseño y coordinación: Laura Barrios
Diseño y diagramación: Karina Domínguez
Edición: Laura Wulichszer
Corrección: Martín Vittón

Las páginas web citadas fueron consultadas entre julio y diciembre de 2019.

Revista Derecho y Nuevas Tecnologías

CeTyS
Universidad de San Andrés

Índice

Agradecimiento

En nombre del Comité Editorial de la Revista de Derecho y Nuevas Tecnologías*, agradecemos a todas las personas que a lo largo de todo este tiempo han hecho posible que la revista crezca en cada nueva edición. A cada uno de los autores y autoras que con su valioso aporte enriquecen nuestra disciplina. A todos los estudiantes que con su entusiasmo e inquietudes nos estimulan a seguir pensando y a emprender proyectos como este. A las autoridades de la Universidad de San Andrés, miembros del Departamento de Derecho y especialmente al equipo del Centro de Estudios en Tecnología y Sociedad (CETyS), gracias por todo el apoyo que siempre nos dan.*

Editorial

El segundo número de la *Revista Derecho y Nuevas Tecnologías* (*RDYNT*) que publica el Centro de Tecnología y Sociedad de la Facultad de Derecho de la Universidad de San Andrés muestra lo variado e interdisciplinario de las áreas que cubre esta publicación: desde el uso de marcas en Internet hasta la firma digital, pasando por los aspectos internacionales del ciberdelito, la violencia de género online y la aplicación de la tecnología a la práctica jurídica que recibe el nombre de *legaltech*.

Dos notas muy interesantes abordan aspectos relacionados con el ciberdelito, en concreto la Cloud Act y el Convenio de Budapest, acuerdo que ahora forma parte de nuestro Derecho interno. Primero, Daniela Dupuy y Mariana Kiefer explican los conflictos que se producen con los pedidos de datos a plataformas en otros países y la sanción de la ley Cloud Act a raíz del caso "Microsoft Ireland". Por su parte, Carla Delle Donne comenta la aprobación del Convenio del Cibercrimen por Argentina y su incorporación al Derecho argentino.

En el tema de responsabilidad civil de intermediarios de Internet, publicamos la sentencia de la Cámara Comercial en el caso "Kosten" y un excelente artículo de Rodolfo Christophersen en el que analiza en detalle este precedente así como otros anteriores.

Por su parte, Lucía Suyai Mendiberri escribe sobre el derecho de supresión en plataformas digitales y la competencia de la AAIP en dicha materia, a la luz de la libertad de expresión y los reconocidos Principios de Manila.

Julián Dunayevich, Gabriela Ramírez, Camila Trentadue, Daniel Franca y Tamara Zylbersztejn escriben una interesante nota que narra la historia de la creación, puesta en marcha y funcionamiento de la entidad registrante de dominios de nuestro país, NIC Argentina.

Las cuestiones fintech y de firma digital también están presentes en una nota de Andrés Chomczyk sobre *smarts contracts*, y en dos notas de Leonor Guini, la primera sobre la identificación digital y la segunda sobre la reciente caducidad de la licencia de un certificador licenciado en la Argentina. Por su parte, Ariel E. Provenzani Casares escribe sobre

la posibilidad de obtener medidas cautelares en base a instrumentos electrónicos privados.

Desde la OMPI, Ignacio de Castro, Leandro Toscano y Gonzalo Bleda colaboran con una nota sobre los mecanismos alternativos de resolución de controversias como herramienta eficaz para facilitar la solución de conflictos en la contratación de software.

También hay tres notas sobre Derecho de marcas. La primera la hemos escrito en conjunto con Guillermo Cabanellas y analiza el *leading case* "Veraz v. Open Discovery", que trata sobre uso de marcas notorias como *keywords* para publicidad en buscadores de Internet y presenta la novedad en la Argentina de resolver la cuestión no solo por el Derecho de marcas sino también por la competencia desleal. Otro comentario al mismo caso está escrito por Javier Alejandro Papaño. La tercera nota aborda las reformas introducidas en el registro de marcas en el INPI, y se centra en la solución de disputas de oposiciones en sede administrativa en vez de la judicial.

En la sección "Seminario" de la revista publicamos la transcripción del debate que tuvo lugar en el seminario *El derecho a la imagen en Internet y la violencia de género en ambientes digitales*. Podemos decir con orgullo que el CETYS de la UDESA fue el primer centro universitario en detectar la importancia de la temática y en organizar una reunión académica donde se debatieron casos reales, incluyendo a las víctimas de estos hechos delictivos y sus abogados, así como fiscales y reguladores que intervinieron en la materia. La conclusión del seminario es que aún queda mucho por hacer.

La sección "Jurisprudencia" contiene el texto completo los casos "Kosten v. Mercadolibre", "Organización Veraz v. Open Discovery" y el caso "Uber" resuelto por el Tribunal de Justicia de la Ciudad Autónoma de Buenos Aires.

Este número de la revista termina con un comentario de Jorge J. Vega Iracelay sobre un libro de *legaltech*. Las herramientas tecnológicas que se están introduciendo en el sector legal, agrupadas bajo el término *legaltech* o *lawtech*, están revolucionando la industria legal al aumentar la velocidad y la eficiencia de los servicios jurídicos tradicionales, o al reemplazarlos en parte con nuevas aplicaciones y formas de prestación. Este

proceso de disrupción en las profesiones jurídicas ofrece oportunidades significativas para todos los actores. Sin embargo, también plantea una serie de desafíos para los profesionales, tanto para los que ejerzan por cuenta propia como para aquellos que estén integrados en despachos o asesorías jurídicas. Esta reciente obra colectiva fue dirigida por el profesor español Moisés Barrio Andrés, autor de varios libros jurídicos sobre las relaciones entre Derecho y tecnología.

Pablo A. Palazzi
Profesor de UDESA
Codirector de CETYS

Doctrina

Marcas y competencia desleal en Internet

por Guillermo Cabanellas y Pablo A. Palazzi

1. Introducción

En esta nota comentamos la decisión de la Cámara Civil y Comercial Federal en el caso "Organización Veraz v. Open Discovery",[1] en sus aspectos más salientes. Primero, el considerar infracción marcaria el uso de una marca por un competidor para generar avisos online; segundo, al juzgar la misma conducta como un acto de competencia desleal; y tercero, al medir los daños por el uso no autorizado de marca y desvío de clientela en función de los datos generados en Internet por el competidor a través del uso de medios de pago online y herramientas de publicidad del buscador.

El fallo que anotamos es un *leading case* en materia de aplicación de Derecho de marcas y competencia desleal en Internet por estos motivos. El resultado es muy positivo para la tutela de las marcas en Internet y reafirma el trabajo señero que los tribunales federales con competencia en marcas vienen desarrollando, correctamente a nuestro juicio, respecto a estas cuestiones.

2. El caso y la decisión judicial

Actora (Veraz) y demandada (Open Discovery) son competidoras en la venta de informes comerciales y ambas ofrecen canales online de venta de dichos productos. La actora tiene más de sesenta años en el mercado, mientras que la demandada se incorporó recientemente y comenzó a operar solo en Internet. Dado que era desconocida en el mercado, la demandada comenzó a usar la marca notoria Veraz como palabra clave para poder aparecer en Internet con anuncios frente a consumidores que buscaban a la actora por su marca.

Se discutía en el caso si la utilización por parte de la demandada de la marca notoria de la actora como palabra clave o *keyword* en el sistema de enlaces patrocinados o *keyword advertising* constituye una infracción

[1] CCCF, Sala III, 4/5/2018, "Organización Veraz S. A. v. Open Discovery s/ cese de uso de marca". El fallo no está firme. Disclosure: el doctor Palazzi asesoró a Veraz en este caso.

marcaria en los términos de la Ley de Marcas N.º 22.362 (de aquí en adelante, LM) y un acto de competencia desleal violatorio del artículo 10 bis del Convenio de París para la protección de la propiedad industrial.

El sistema de publicidad online funciona —en forma simplificada—, de la siguiente manera:[2] cada vez que un usuario tipea una palabra en un buscador de Internet, además de los resultados de búsqueda orgánicos suelen aparecer resultados patrocinados (avisos comerciales), que son generados a partir de las palabras clave pagas que los anunciantes ingresan en el sistema de búsqueda. A veces esas palabras pueden ser signos marcarios registrados y el anunciante puede ser un competidor del titular marcario, que estaría usando la marca para generar publicidad comercial a su favor con la ventaja de que solo ven esa publicidad quienes buscan el producto de su competidor en Internet.

En este caso la actora demandó a un competidor que usaba la marca notoria de la actora para generar avisos patrocinados online que llevaban al sitio de la demandada, donde solo con un par de clics era posible comprar un informe comercial de contenido similar al de la actora. Este desvío de clientela generó una acción por infracción marcaria y también por competencia desleal. En su demanda, la actora dejó en claro que demandaba sobre la base de ambos regímenes de protección, en forma independiente y no subsidiaria.

Ambas instancias judiciales condenaron a la demandada. En primera instancia se hizo lugar a la demanda y se condenó a indemnizar los daños por el uso no autorizado de la marca notoria Veraz[3]. Ambas partes apelaron. La actora apeló por considerar bajo el monto de condena y por no haberse aplicado también las normas de competencia desleal. La demandada apeló alegando que *(i)* no había uso marcario porque la marca no se veía, *(ii)* que la marca Veraz era genérica y *(iii)* que se usaban numerosas palabras clave, no solo la marca Veraz. La cámara confirmó la condena

[2] Para una explicación detallada del funcionamiento puede verse el fallo anotado, punto V y también: Cabanellas de las Cuevas, Guillermo, y Palazzi, Pablo, "Derecho de Internet en Argentina", en *Derecho de Internet*, Cabanellas de las Cuevas (dir.), Buenos Aires, Heliasta, 2004, pp. 44-45; y Palazzi, "El uso no autorizado de marcas en publicidad en buscadores y la inmunidad de los intermediarios de Internet", *LL* 2010-E-215.

[3] Juzgado Civil y Comercial Federal N.º 2, sec. 3, expte. N.º 1789/2009, 16/6/2017, "Organización Veraz S. A. v. Open Discovery s/ cese de uso de marca".

con extensos fundamentos, agregando la existencia de competencia desleal como un motivo separado de la infracción marcaria. Asimismo, la alzada elevó el monto de la condena patrimonial en función de la prueba informática producida en el expediente[4].

3. Derecho de marcas y nuevas tecnologías

En las últimas décadas, Internet pasó de ser una colección de redes académicas usadas por universidades para investigación a transformarse en una red eminentemente comercial,[5] siendo un verdadero motor de nuevos negocios. Nace así el concepto de comercio electrónico. Con la aparición de este comercio virtual, llegaron también los problemas legales relacionados con las marcas en el mundo online.

Internet creó un nuevo mercado donde las marcas juegan un papel cada vez más importante. Las ventas en Internet son cada vez mayores, y la publicidad online ha desplazado a la publicidad a través de los canales tradicionales. Los actores de Internet se han transformado en verdaderos gigantes multimedios, superando en su valuación patrimonial a las empresas convencionales e incluso a varios países[6]. Las empresas han dirigido su presupuesto a la pauta online dejando de lado el aviso en formato papel. A tal punto, que la falta de inversión en publicidad tradicional ha impactado fuertemente en los ingresos de los diarios[7]. Hoy en día, Internet es un verdadero motor del comercio mundial, que crea nuevas industrias y, al mismo tiempo, que destruye otras antiguas que no saben amoldarse a los cambios.

Ante tal panorama, es normal que se incrementen los usos marcarios online y que también lo hagan las infracciones en dicho medio, ya que este es el lugar donde se desarrolla la lucha por el cliente.

---

[4] CCCF, Sala III, 4/5/2018, "Organización Veraz S. A. v. Open Discovery s/ cese de uso de marca".

[5] Ver Greenstein, *How the Internet Became Commercial. Innovation, Privatization, and the Birth of a New Network*, Princeton University Press, 2015.

[6] Ver "Associated Press, Apple, Amazon, Facebook, Alphabet, and Microsoft Are Collectively Worth More Than the Entire Economy of the United Kingdom", April 2018; Surowiecki, James, "Why Tesla Is Worth More Than GM", MIT Technology Review, 27/6/2017.

[7] Saperstein, "The Future of Print: Newspapers Struggle to Survive in the Age of Technology", Harvard Political Review, 6/12/2014.

Cada vez con mayor frecuencia veremos que los litigios relativos al uso no autorizado de signos distintivos van a tener un aspecto relacionado con el mundo online, y en algunos casos, como el que anotamos, la infracción se habrá producido en el mundo online exclusivamente. Un aspecto importante a considerar entonces es que lo que sucede en el mundo online no ocurre en un espacio virtual alejado de la realidad, sino que tiene impacto directo en las elecciones de los consumidores y en el bolsillo de empresas que operan en este nuevo medio. Por otra parte, la mayoría de las leyes vigentes y principios generales del Derecho siguen resultando aplicables al mundo virtual.

Un claro ejemplo es el caso que anotamos, en el que una empresa desconocida hasta su aparición en el mercado de informes comerciales comenzó a operar exclusivamente online y, para captar clientela, empezó a usar las marcas de sus competidores (varios de ellos, no solo de la actora) en avisos online. Esta práctica es cada vez más frecuente y ya ha generado numerosos litigios en el Derecho Comparado[8].

4. Uso de marcas en enlaces patrocinados

Respecto a la decisión del tribunal, haremos comentarios relativos a: *(i)* la aplicación del Derecho Marcario al uso de palabras clave para generar publicidad, y *(ii)* la aplicación de la competencia desleal a litigios marcarios.

4.1. Enlaces patrocinados como infracción marcaria

El fallo que anotamos concluyó que el competidor demandado usaba la marca de la actora para generar publicidad online y ello constituía infracción marcaria, conclusión que compartimos.

Se han esbozado varios argumentos para evitar la aplicación del Derecho de Marcas al uso de signos distintivos para generar enlaces patrocinados. Los podemos resumir en estos tres:

[8] Palazzi, "El uso de marca ajena en enlaces patrocinados en buscadores de Internet", *Derechos Intelectuales*, N.º 16, pp. 39-71. ASIPI, Legis, 2011.

(i) no hay uso marcario típico o uso en el tráfico comercial ya que se trata de un simple uso interno;

(ii) no hay confusión marcaria;

(iii) estos usos de la marca permiten más opciones al consumidor, y es propio del Derecho de Marcas informar al consumidor para generar más competencia.

Respecto a la *falta de uso marcario típico*, la respuesta a este argumento es que los usos marcarios atípicos también pueden ser infracciones marcarias, y las *keywords* podrían entrar en esta categoría.

La doctrina[9] ha diferenciado el uso marcario en *típico* y *atípico*, también llamado *uso marcario* y *uso no marcario*.

El uso marcario típico es aquel que afecta la función esencial de la marca que es la distintiva. Consiste en usar de alguna forma la marca en el tráfico comercial para indicar el origen de un producto. En la Argentina, el uso atípico se analiza sobre la base de conceptos generales del Derecho de Marcas. Así, cuestiones tales como el uso de la marca en publicidad, en papelería, anuncios y prospectos, o respecto de la prestación de servicios, son tratados por la doctrina argentina como supuestos de aplicación del artículo 31 de la LM. Las sanciones aplicables a los ilícitos marcarios se reservan a aquellos supuestos en que una conducta vulnera las funciones esenciales y jurídicamente protegidas como tales de los signos marcarios, mientras que los casos en que la conducta no configura tal vulneración pero sí una situación de competencia desleal son tratados bajo las normas específicas relativas a este último caso.

A su vez, el uso marcario atípico puede ser legal o ilegal. Como los usos atípicos marcarios entran en una zona gris, a veces suelen ser resueltos mediante las reglas relativas a la competencia desleal[10]. Un claro ejemplo de uso marcario atípico legal es la publicidad comparativa, que se considera en la mayoría de los supuestos legal desde el punto de vista

[9] Estas dos especies no constituyen categorías jurídicas con efectos inmediatos, más bien se trata tan solo de instrumentos destinados a orientar la determinación de los límites de la licitud del uso de signos marcarios ajenos. Para mayor detalle, ver Cabanellas de las Cuevas, "El uso atípico de la marca ajena", *Temas de derecho industrial y defensa de la competencia*, N.º 3, p. 44 y ss.

[10] Cabanellas de las Cuevas, "El uso atípico de la marca ajena", op. cit., y Cabanellas de las Cuevas, Serebrinsky, Sánchez Herrero y Palazzi, *Derecho de la competencia desleal*, p. 445.

marcario, pero en muchos casos encuentra sanción en la competencia desleal[11].

Así sucede también con otros supuestos tales como la imitación desleal por riesgo de confusión, con los actos susceptibles de crear confusión bajo el artículo 10 bis del Convenio de París, con ciertos usos atípicos marcarios y con la publicidad comparativa de carácter desleal o denigratoria[12].

En síntesis, se aprecia como bastante simplista el argumento de que no hay uso de marca porque esta no se encuentra fijada en producto o servicio alguno. En todo caso, podría aclararse que el uso no es típico sino atípico pero ilegal. Se podría sostener que, al incluir la marca como una *keyword* para generar publicidad justo en el momento en que el consumidor busca la marca de la actora, se está haciendo un uso atípico de la marca para publicidad por sus efectos. Es un claro uso no autorizado, que el titular tiene derecho a prohibir. Máxime si quien así la usa es un competidor que se aprovecha de la marca para una publicidad comercial donde se ofrecen productos en competencia directa. Frente al avance de las nuevas tecnologías, los criterios de infracción marcaria deben ser más flexibles, y esta es la línea que sigue el tribunal en el caso que anotamos.

Al respecto, la doctrina marcaria argentina que ha comentado este mismo caso anotado sostuvo: "La adopción de una marca ajena como palabra clave por parte de un competidor constituye un ilícito marcario, y como tal, un acto de competencia desleal, susceptible de generar el deber de reparar los perjuicios causados"[13]. En igual sentido se pronunció la jurisprudencia norteamericana[14].

Distinto es el caso de un mercado virtual, que usa la *keyword* para informar la presencia de ciertos productos en su plataforma online. Este parece ser un uso referencial más que un uso competitivo[15]. En principio, si el mercado virtual vende productos legítimos u originales, este tiene

[11] Palazzi, "Evolución de la jurisprudencia argentina en materia de publicidad comparativa", *RDCO*, 2010-B-717.

[12] Cabanellas de las Cuevas et al., *Derecho de la competencia desleal*, pp. 304-305, 425-443, 445-467 y 401-424.

[13] Papaño, Javier, "Buscadores de Internet, palabras clave y uso de marca ajena", *LL* 2018-D-153.

[14] Caso "Rescuecom Corp.", 562 F.3d 130.

[15] Luski, Gisela, "El uso de marcas ajenas en publicidad online", *Revista Iberoamericana de la Propiedad Intelectual*, t. 4, 2016, p. 263.

derecho a informarlo al público con mención de los datos que identifican al producto incluyendo la marca. Pero si un mercado virtual deja de tener un rol neutro y pasa a tener un rol activo en la infracción marcaria, y usa la *keyword* para llevar al consumidor a productos falsificados con conocimiento de causa, entonces no parece ser un uso lícito de la marca[16].

Por otra parte, si cuando el internauta llega al sitio a través de esa publicidad y se encuentra con productos de la competencia, y ninguno de los productos que se infieren del aviso online, entonces parece ser un caso de *click and bait* o de decepción al consumidor. Estos son casos donde se atrae al consumidor, quien espera encontrar una marca y luego encuentra otra que ofrece productos sustitutos. Cierta jurisprudencia encasilla estos casos en la doctrina de la *initial interest confusion*.

Como señalamos al inicio, es frecuente también el argumento de la *falta de confusión en el uso de keywords*. Se argumenta que la marca aparece y se usa porque la tipea el usuario, y a raíz de esta acción del usuario de Internet (y el hecho de que el competidor la incluyó en la base de datos de anuncios), aparece el aviso del competidor. De esa manera, el usuario no podría confundirse.

En primer lugar, lo que se puede responder a este argumento es que la confusión debe analizarse caso por caso y no es posible afirmar en abstracto que en determinados casos no existe confusión. Por otra parte, es importante recordar los principios legales en la materia cuando se usa la misma marca para la misma clase de productos. Es que el artículo 16 del Acuerdo sobre Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio (ADPIC) claramente identifica como infrac-

[16] CCCF, Sala 1, causa N.º 2060/2008, "Nike International Ltd. c/ DeRemate.com de Argentina S. A. s/ Cese de uso de marcas y daños y perjuicios", 5/5/2015; Cámara Nacional de Apelaciones en lo Civil y Comercial Federal, Sala 3, causa N.º 3239/2007, "Nike International Ltd. c/ Compañía de Medios Digitales CMD S. A. s/ Cese de uso de marcas", 21/5/2015, donde se concluye que ambos demandados son responsables por infracción de marcas al permitir que los usuarios de sus plataformas electrónicas vendieran productos Nike falsificados. En el caso ambos tribunales concluyeron que tanto DeRemate como CMD no eran meros intermediarios neutrales sino que tuvieron un papel activo. En esa línea de ideas, y citando el *leading case* "L'Oréal c/ eBay" decidido por el Tribunal Europeo de Justicia se sostuvo que DeRemate tuvo un papel activo ya que *(i) compró el término "Nike" como palabra clave para redirigir a los usuarios* a su sitio web y *(ii)* les brindaba a sus usuarios un método de pago que facilitaba las transacciones. La Cámara de Apelaciones también encontró que CMD tuvo un papel activo toda vez que ayudó a promover los productos en infracción y cobró una comisión por cada operación realizada.

ción marcaria los casos de doble identidad, al disponer: "El titular de una marca de fábrica o de comercio registrada gozará del derecho exclusivo de impedir que cualesquiera terceros, sin su consentimiento, utilicen en el curso de operaciones comerciales signos idénticos o similares para bienes o servicios que sean idénticos o similares a aquellos para los que se ha registrado la marca, cuando ese uso dé lugar a probabilidad de confusión. En el caso de que *se use un signo idéntico para bienes o servicios idénticos*, *se presumirá que existe probabilidad de confusión*".

Aplicando ese principio al caso que anotamos, podemos afirmar que el uso en el comercio (en el caso, en publicidad online) de una marca idéntica a la del titular marcario para los mismos bienes (informes comerciales) autoriza a presumir la confusión marcaria. De alguna forma esto tiene lógica y explica por qué se paga y se usan tanto las *keywords* relacionadas con marcas en los avisos online[17]. De acuerdo con el artículo 16 del ADPIC, el demandado debe entonces demostrar esa falta de confusión[18].

Incluso la doctrina no ya legal sino del área de marketing que ha estudiado el tema, señala que la confusión dependerá también de cómo el buscador separa los resultados orgánicos de los auspiciados o pagos, lo cual está sujeto a posibles cambios a futuro e íntimamente unido al modelo de negocios de los buscadores. Esto podrá influir en cómo el usuario ve ambos resultados y si es capaz o no de diferenciarlos[19].

En segundo lugar, el titular de una marca tiene derecho a obtener el cese de uso no autorizado de su marca cuando esta es usada para generar anuncios por parte de un competidor para los mismos bienes y servicios. El titular marcario no tiene por qué esperar a que exista un caso de confusión marcaria si quien la usa es justamente un competidor y tal uso lesiona su derecho sobre la marca.

En tercer lugar, el titular marcario tiene derecho a prohibir el uso de su marca en una base de datos que va a generar avisos comerciales a favor

[17] Talbot, "Working With Trademarks in PPC", *Medium*, 23/2/2017 [https://bit.ly/2TJGFXC].
[18] La doctrina sostiene en que el art. 16 del ADPIC invierte la carga de la prueba en los casos de doble identidad. Ver Stoll, Peter Tobias, y otros, *WTO-Trade-related Aspects of Intellectual Property Rights (Max Planck Commentaries on World Trade Law)*, Martinus Nijhoff, p. 319.
[19] Ver Goodstein, Ronald, Gary J. Mossy, Basil G. Englis & Howard S. Hogan, "Using Trademarks as Keywords: Empirical Evidence of Confusion", *The Trademark Reporter*, May-June, 2015, vol. 105, N.º 3.

de un competidor. La inclusión de esta *keyword* en una base de datos no es un uso privado o interno sin efectos comerciales. El uso de la marca en esta base de datos es un uso no autorizado del signo del mismo modo que en el pasado se consideraron ilegales otros casos similares, como ser *(i)* uso pasivo de nombres de dominio y *(ii)* uso de metatags dentro del código HTML de una página web.

Veamos el caso del uso pasivo de nombres de dominio de Internet, esto es, del registro de un nombre de dominio por un tercero sin uso activo del mismo y sin dotar de contenido el nombre de dominio. En estos casos siempre se concluyó que el mero registro del nombre de dominio idéntico a la marca era ilegal[20]. Esta situación es análoga al caso que comentamos y nunca se cuestionó su lógica.

El otro ejemplo de uso de marcas en forma ilegal cuando estas *no son visibles* por el consumidor son los metatags insertos en la página web de un competidor[21]. El metatagging era una práctica empleada por los operadores de ciertas páginas web con el propósito de captar la atención de los usuarios de Internet mediante un sutil empleo de marcas ajenas. Esta práctica consiste, en particular, en incluir en el código HTML —en el lenguaje de redacción y formateo empleado en una página de Internet y, por lo tanto, de forma no perceptible para el ser humano—, la marca, el nombre u otro signo distintivo de un tercero en el apartado de palabras clave de la propia página web (*metatag keyword section*). La información contenida en el metatag es empleada por las herramientas de búsqueda usadas en Internet para clasificar las direcciones de los diversos recursos localizados en la red y así para identificar y ordenar la dirección en cuestión en la base de datos que los operadores de las herramientas de búsqueda ponen a disposición de sus usuarios. De esta manera se logra crear confusión en el público, pues ciertamente invita a establecer una conexión entre el resultado de la búsqueda y la procedencia empresarial de ese resultado; no parece difícil que el público tienda a pensar que ese resultado de la búsqueda contiene información u ofertas sobre los productos o servicios distinguidos con la

[20] Palazzi, "La protección internacional de los nombres de dominio", *ED*, 242-690, donde se desarrollan en extenso los casos resueltos bajo la UDRP que consideran infracción marcaria el uso pasivo de nombres de dominio.

[21] Massaguer, José, "Las marcas en Internet", *Derecho de Internet*, op. cit., pp. 236-240.

marca o que ha sido confeccionada por una persona relacionada o autorizada por el titular de la marca.

Cabe señalar que numerosos tribunales extranjeros han considerado ilegal esta práctica dentro de las normas de la propiedad industrial[22].

Lo cierto es que, aunque la marca no se vea, en los casos de uso de marca como metatags se condenó dicha práctica. En 1997 comenzó a discutirse la legalidad de esta conducta. El primer caso involucró nada menos que a un estudio jurídico de marcas que vio su signo distintivo y nombre comercial usado sin permiso como metatag en varios sitios de terceros. En el caso "Oppedahl & Larson v. Advanced Concepts"[23] el tribunal ordenó el cese de la conducta. El mismo año otro tribunal dictó una sentencia firme en la que concluyó que el uso de la marca de un tercero como metatag era infracción marcaria y que el único motivo por el cual podría usar dicha marca era para atraer ilícitamente tráfico a su web[24].

La tesis se sigue manteniendo, como lo demuestra este reciente caso del año 2018 en "Adidas America v. Skechers". En este caso, la demandada utilizó como metadato el término "Adidas Stan Smith" en su sitio web. La empresa Adidas ofrece a la venta una zapatilla auspiciada por el jugador de tenis Stan Smith. Un dato adicional del caso es que la tienda demandada ofrecía una zapatilla confundible con el *trade dress* de la zapatilla de la actora llamada Skechers Onix. El demandado fue condenado en primera instancia por infracción marcaria. La demandada apeló. La Cámara de Apelaciones del Noveno Circuito, en un fallo contundente, concluyó: "*We agree with the district court that the only reason 'Adidas Stan Smith' is a useful search term is that consumers associate the term with a distinctive and recognizable shoe made by Adidas*"[25].

---

[22] Ver fallos citados por Massaguer, op. cit., p. 237; ver también Cabanellas de las Cuevas y Palazzi, "Derecho de Internet en Argentina", op. cit., pp. 44-45, donde se lo considera acto de competencia desleal.

[23] Caso "Oppedahl & Larson v. Advanced Concepts", Civ. No. 97-Z-1592 (D. C. Colo., July 23, 1997).

[24] Caso "Insituform Technologies Inc. v. National Envirotech Group, L.L.C.", Civ. No. 97-2064 (E. D. La., final consent judgment entered Aug. 27, 1997). En el mismo sentido ver "Playboy Enterprises Inc. v. Calvin Designer Label", Civ. No. C-97-3204 (N. D. Cal., Sept. 8, 1997) (medida cautelar de cese de uso de marca emitida contra un competidor).

[25] Cámara de Apelaciones del Noveno Circuito, caso "Adidas America, Inc. v. Skechers USA, Inc.", No. 16-35204 (9th Cir. May 10, 2018).

Es evidente entonces que cuando se usan estos términos, no se lo hace en sentido nominal o no marcario, sino con el fin de atraer clientela que busca ese término, y justamente ello implica usar la marca para generar confusión en el consumidor, aunque sea inicial.

Finalmente, respecto al *argumento competitivo y la generación de mayor información*, podemos responder que la indicación de origen de un producto, que es la función primordial de la marca, implica indicar el origen por parte del propio comerciante, pero no implica que el competidor pueda usarla con el objeto de acercarse a los clientes de sus competidores en el momento de la búsqueda "para brindarles mayor información".

Por otra parte, la Ley de Marcas vigente en la Argentina no da valor jurídico autónomo a la función competitiva o concurrencial de las marcas[26]. Es cierto que la función de las marcas no se agota en la tutela de las empresas respecto de situaciones calificables como de competencia desleal. Los signos marcarios están también destinados a facilitar la comparación entre sí de los distintos productos ofrecidos[27]. Un ejemplo de ello es la publicidad comparativa, donde el uso de la marca podrá ser legal desde el punto de vista marcario, pero ilegal desde el punto de vista de las normas de la lealtad comercial o la competencia desleal. Sin embargo, en modo alguno este caso era un caso de publicidad comparativa pues no se comparaban ambos productos. Más bien se usaba una marca notoria para desviar clientela online.

Se advierte que, en parte como consecuencia de la propia evolución histórica del régimen de marcas y de Internet, existen en el marco de esta última múltiples conductas que no encuadran en las categorías originalmente desarrolladas por aquel. En el presente caso, desde el punto de vista del Derecho de Marcas "clásico", existe un uso atípico de la marca por cuanto la demandada no la utilizaba para identificar sus propios bienes o servicios. Pero sí lo hacía de un modo tal que, por una parte, estaba destinado a desviar la clientela atraída por la marca de la actora; por ello se estaba ante un uso parasitario del valor de atracción de clientela de esa marca. Asimismo, la demandada, con los vínculos electrónicos creados

[26] Bertone y Cabanellas de las Cuevas, *Derecho de marcas*, t. 1, p. 68, Heliasta, Buenos Aires, 2003.

[27] Bertone y Cabanellas de las Cuevas, *Derecho de marcas*, op. cit., p. 69.

entre la marca de la actora y sus bienes y servicios, creaba la probabilidad de que el público asociara esa marca —de reconocido valor— y los mencionados bienes y servicios, nuevamente incurriendo en un comportamiento parasitario, además de engañoso. Se violaban así las premisas funcionales del sistema de marcas, y se utilizaban estas para lograr resultados frontalmente opuestos a esas premisas.

4.2. Enlaces patrocinados como competencia desleal

El fallo que anotamos también concluyó que el competidor incurre en competencia desleal cuando usa la marca de la actora para generar publicidad online y efectuar desvío de clientela.

En concreto, el voto de la doctora Medina señala: "[…] la demandada ha incurrido en competencia desleal por cuanto mediante la utilización de la marca notoria de la actora ha procurado captar clientes y desviarlos en favor suyo. Insisto con remarcar que ambas compiten en el mismo mercado y que esta circunstancia es fundamental para resolver el caso. También insisto en remarcar que el link de la accionada aparecía en los primeros lugares de la búsqueda (como enlace patrocinado) justo cuando los usuarios de Internet realizaban la búsqueda insertando la marca notoria de la actora".

En materia de *adwords*, la competencia desleal ha sido aplicada en diversos casos europeos y de otras jurisdicciones. Entendemos que esta actividad puede ser un acto de competencia desleal cuando se usa con conocimiento la palabra clave de un competidor para desviar clientela. Ello es así pues cabe dentro de la definición que da el artículo 10 bis del Convenio de París, que dispone que es tal "todo acto de competencia contrario a los usos honestos en materia industrial o comercial".

En el caso entendemos que no parece honesto ni leal usar una marca notoria de un competidor, así como un nombre comercial ajeno, sin tener autorización legal del verdadero titular. No forma parte de la ética que se espera de un comerciante honesto. Más grave aún es usarlo cuando la marca pertenece a un competidor, y en el caso se trataba de una empresa líder en el rubro, y la marca se usa con el único fin de "subirse al caballo" del éxito ajeno, apropiándose de todo el valor de la inversión realizada en el nombre y la marca de la actora. Resulta un claro caso de explotación de

la reputación ajena. Recordemos que un criterio básico para determinar el carácter leal de una conducta competitiva es que la actuación y el éxito en el mercado se logren mediante la calidad y el precio de las propias prestaciones;[28] en contraposición, es desleal la que implica posicionarse en el mercado mediante el aprovechamiento del esfuerzo ajeno, el engaño y la destrucción de la capacidad productiva de otros competidores. En el caso aquí analizado, la parte demandada utilizaba un mecanismo mediante el cual desviaba en su provecho el prestigio y el poder de atracción de los signos distintivos de su competidor: lograba una ventaja competitiva desviando hacia sí a la potencial clientela de una marca líder, e incluso induciendo a un posible engaño a parte de los consumidores.

En el Derecho Comparado encontramos numerosos casos en los cuales se cataloga como competencia desleal al uso de marcas ajenas para generar publicidad mediante clics de *adwords*.

Así, en Francia la Corte de Apelaciones de París, en el caso "Cobrason c/ Société HomeCinéSolutions",[29] consideró que el uso del nombre comercial de la actora y el nombre de dominio como referencias online implicaba un supuesto de concurrencia desleal y publicidad ilícita con fecha del 11 de mayo de 2011. Esta conclusión no fue alterada por el fallo "Google France" que en la Unión Europea consideró que un intermediario de Internet no era responsable por la inmunidad que tiene como proveedor de servicios de la sociedad de la información, pero sí lo podía ser un competidor que usara la marca como *keyword* bajo las normas de competencia desleal. Ello es así pues el Tribunal Europeo de Justicia solo emite decisiones sobre Derecho Comunitario europeo, pero no se pronuncia sobre temas de competencia desleal, que todavía no es materia armonizada en la Unión Europea[30].

En este caso, la Corte de Apelaciones de París duplicó la condena de primera instancia de 50.000 euros y la elevó a 100.000 euros teniendo en cuenta que se había verificado que 1.257 internautas habían hecho clic en el anuncio en el plazo de seis meses. Respecto a la demandada, el

[28] Cfr. al respecto Cabanellas de las Cuevas y otros, *Derecho de la competencia desleal*, op. cit., caps. I y VI.
[29] Corte de Apelaciones de París, 11/5/2011, "Cobrason c/ Société Home Ciné Solutions".
[30] Cabanellas de las Cuevas y otros, *Derecho de la competencia desleal*, op. cit., p. 110.

tribunal concluyó que: "[…] *la Société HomeCinéSolutions, en utilisant la dénomination sociale et le nom de domaine d'un concurrent a nécessairement généré une confusion dans l'esprit de la clientèle potentielle des deux sites et provoqué de ce fait outre un détournement de cette clientèle, une utilisation parasitaire des investissements de la société Cobrason (investissements visant tant le site internet que l'organisation de campagnes publicitaires)*".

El tribunal hace alusión a la competencia parasitaria, que es una modalidad de aprovechamiento injusto del esfuerzo ajeno, reconocido en algunos países europeos y contenida en la cláusula general del artículo 10 bis del Convenio de París[31]. En Francia la figura de competencia parasitaria ha sido reconocida por la doctrina[32] y elaborada por numerosos casos judiciales[33].

En el mismo sentido un tribunal de Estrasburgo, en el caso "Francia Atrya v. Google, et al.",[34] consideró que incurre en competencia desleal —en la subespecie de actos de parasitismo— el anunciante que para atraer clientela en Internet a sus propios productos utilizaba la marca de su competidor en anuncios, dado que el parasitismo se caracteriza por obtener ganancias aprovechándose del prestigio y notoriedad de su competidor.

Cabe recordar que en Francia no existe una ley general de competencia desleal y la jurisprudencia se basa en la obligación genérica de no dañar contenida en el Código Civil Francés[35]. Justamente de esto se tratan los reclamos de competencia desleal: de obtener una indemnización por los daños irrogados a la parte afectada por los actos de un comerciante desleal[36]. En la Argentina, si bien no existe una ley general de competencia desleal, está vigente la Convención de París, cuyo artículo 10 bis recepta la cláusula general de competencia desleal que tiene efecto directo en nuestro ordenamiento jurídico y sirve para fundar las ilegalidades en materia de aprovechamiento injusto del esfuerzo ajeno.

En Italia la jurisprudencia también se ha inclinado por la competencia desleal (en vez de la infracción marcaria) para condenar el uso

[31] Ver OMPI, *Protección contra la competencia desleal*, Ginebra, 1994, p. 65.
[32] Malaurie-Vignal, M., "Parasitisme et notoriété d'autrui", *JCP* 1995, I, 3888; Reisch, O., "Concurrence déloyale et parasitisme: Régime", *Encyclopédie juridique des Biens informatiques*, 29 juin 2004.
[33] Cour d'appel de Paris, 4ème ch., 8 septembre 2004 SFR et Publicis Conseil c/ Besson et Gaumont.
[34] Corte de Apelaciones de Estrasburgo, 20/7/2007, "Francia Atrya v. Google, et al.".
[35] Cabanellas de las Cuevas y otros, *Derecho de la competencia desleal*, op. cit., p. 102 y ss.
[36] Cabanellas de las Cuevas y otros, *Derecho de la competencia desleal*, op. cit., p. 842.

abusivo de *keywords* en numerosos precedentes[37]. Un tribunal de Milán (sentencia del 11 de marzo de 2009) concluyó que "*E' concorrenza sleale il comportamento della società che aggancia parassitariamente il proprio sito internet al marchio di una società concorrente*". Un tribunal de Nápoles llegó a la misma conclusión que el tribunal francés antes citado[38].

Finalmente, en el caso chino "Beijing Orient Qingruan Science and Technology Co., Ltd v. Beijing Langde North Software Education Technology Co., Ltd.", un tribunal de Beijing concluyó, en julio de 2010, que el demandado, competidor de la actora, era culpable de competencia desleal por usar la marca como *keyword* para generar publicidad online.

5. Conclusiones

El fallo dictado por la Sala III de la Cámara Civil y Ceomercial es impecable. No tiene desperdicio en ninguno de sus párrafos. Sanciona una conducta que es desleal, realizada por un competidor mediante el uso de la tecnología como una forma de "subirse" al prestigio de una marca notoria y lograr de esa manera la atención del público consumidor, no por las virtudes del producto sino a través de artilugios tecnológicos.

Internet apareció en 1990 como un nuevo medio de comercialización (si bien ya funcionaba desde 1969) pero rápidamente este canal empezó a absorber a los otros canales, diluyendo la publicidad tradicional y obligando a invertir en publicidad online, creando nuevos problemas legales con los nombres de dominio, el uso de marca como metatag o como *keyword*, la venta de productos falsos en redes sociales, la creación de espacios de la marca en redes sociales y un largo etcétera.

Desde el primer caso resuelto sobre esta temática hace casi dos décadas —caso Freddo.com.ar— hasta este precedente, el fuero civil y comercial federal ha demostrado una gran comprensión de las nuevas

[37] Ver Tribunale di Roma, fallo del 18/1/2001 con comentario de R. Sciaudone in Riv. Dir. Ind. 2002, II, 189 y de P. Sammarco in Dir. Inf. I, 2001; ver asimismo Trib. Milano 8/2/2002 in AIDA 2002 y Trib. Napoli 28/1/2001 en Dir. Inf. 2002 y Tribunale delle Imprese di Venezia, caso "Obiettivo Risarcimento S. R. L.".

[38] Tribunale di Napoli, Sezione specializzata in materia d'impresa, ordinanza 17/6/2014.

tecnologías y la posibilidad de adaptar el Derecho de la Propiedad Intelectual para amparar nuevas situaciones infractoras.

Por ejemplo, la Cámara Federal ha dictado importantes precedentes que tutelan la venta de productos falsificados online, como ocurrió en el caso "Nike v. Deremate" y "Nike v. CMD"[39]. También supo poner límites al uso del Derecho Marcario en nombres de dominio, como ocurrió en el caso "quetepasaclarín.com"[40]. Y ahora en este precedente vuelve a aplicar el Derecho Marcario (con una ley marcaria antigua pero sólida) a Internet, logrando un resultado positivo. El fallo que anotamos resuelve el debatido caso de las *adwords* y lo hace de una forma que permite respetar la vigencia de la marca en Internet.

La figura de competencia desleal ha sido utilizada, tanto en este como en otros casos, para superar posibles dudas respecto del alcance de las infracciones marcarias propiamente dichas. Debe observarse, sin embargo, que este desplazamiento en la calificación de conductas relativas a marcas no es carente de efectos. No son iguales las sanciones ni el procedimiento relativo a infracciones marcarias que el propio de la competencia desleal. Cabe entonces preguntarse si no sería más razonable efectuar una interpretación más amplia de las figuras marcarias, extendiéndolas como tales a conductas relativas a marcas ajenas que —posibilitadas por las técnicas actuales— difieren del uso típico de la marca, pero que tienen un contenido esencialmente marcario, por cuanto implican aprovechar el prestigio y el poder de atracción de marcas ajenas. El texto de la Ley N.º 22.362 es suficientemente amplio para abarcar estos usos de marcas ajenas que, más que atípicos, cabría hoy calificar de novedosos.

[39] CCCF, Sala 1, Causa N.º 2060/2008, 5/5/2015, Nike International Ltd. c/ DeRemate.com de Argentina S. A.; CCCF, Sala 3, Causa N.º 3239/2007, 21/5/2015, "Nike International Ltd. c/ Compañía de Medios Digitales CMD S. A. s/ Cese de uso de marcas".
[40] CCCF, Sala III, 11/2/2014, "Arte Gráfico Editorial Argentino S. A. c/ Castañeda, Matías".

La transferencia transfronteriza de datos en el marco de investigaciones criminales

por Daniela Dupuy y Mariana Kiefer

Resumen: Hoy en día resulta necesario, en el marco de las investigaciones penales, contar con cierta información digital que se encuentra en poder de los proveedores del servicio de comunicaciones electrónicas por Internet. Esas compañías se ubican —en la mayoría de los casos— fuera de la Argentina. Los instrumentos de cooperación internacional tradicionales han demostrado su ineficacia como medio para obtener la información de manera oportuna y ágil. Esas circunstancias han sido debatidas en el caso Microsoft/Irlanda, cuyo desenlace ha sido observado desde todo el mundo. A raíz del caso, Estados Unidos sancionó recientemente una ley que intenta dar respuesta a este nuevo desafío que presentan los desarrollos tecnológicos, poniendo en pugna la persecución penal del Estado *Conclusiones* la protección de datos y el derecho a la privacidad y a la intimidad.

Palabras clave: cooperación internacional, MLAT, evidencia digital, Cloud Act, caso Microsoft/Irlanda.

Title: The new Cloud Act: Its impact on investigations carried out in digital environments.

Abstract: Nowadays, in the context of criminal investigations, it is necessary to have access to certain digital data which are in the hands of Internet Service Providers. These companies are based mostly out of Argentina. Traditional International Cooperation instruments have proven ineffective as a means to obtain said information in a timely and agile fashion. These circumstances have been discussed in *Microsoft/Ireland*, the results of which were followed all over the world. As a consequence, the US have recently passed a new law which aims at providing answers to the new challenge posed by technological developments, in which the government criminal prosecution is in tension with the protection of data and the rights to privacy.

Keywords: International Cooperation, MLAT, digital evidence, Cloud Act, Microsoft/Ireland.

1. Planteamiento del problema

Los esfuerzos para proteger a la ciudadanía y combatir la delincuencia grave se han visto obstaculizados por la imposibilidad de acceder a datos almacenados fuera de Estados Unidos y que se encuentran en custodia de las empresas proveedoras de servicio de Internet, sujetos a la jurisdicción de ese país.

Asimismo, los gobiernos extranjeros también buscan, cada vez más, acceder a datos electrónicos en poder de las empresas de tecnología en Estados Unidos para combatir delitos, toda vez que este se ha convertido en un país central, por encontrarse allí la mayoría de los proveedores de servicios de Internet.

Las empresas de tecnología y comunicación se enfrentan a potenciales conflictos legales cuando los gobiernos piden datos que podrían colisionar con las leyes extranjeras.

La promulgación de la ley denominada Cloud Act[1] propone acuerdos internacionales entre países que resolverían estos conflictos, con el compromiso de respetar la protección de la privacidad y las libertades civiles de los usuarios.

La Cloud Act[2] es una ley federal de Estados Unidos promulgada el 23 de marzo de 2018. La norma fue presentada en febrero pasado ante el Congreso de Estados Unidos por una comisión compuesta por miembros de diferentes partidos norteamericanos. Sin embargo, su aprobación se ha producido sin ningún debate, y fue introducida como parte de la Consolidated Appropriations Act. 2018, una enorme ley presupuestaria de más de dos mil doscientas páginas de extensión, destinada a tratar el cierre financiero del gobierno federal, y se puede encontrar en la última sección la ley de referencia.

[1] La traducción literal sería "Ley de la Nube". Sus siglas en inglés significan Ley Aclaratoria del Uso Legal de Datos en el Extranjero (*Clarifying Lawful Overseas Use of Data*). De ahora en más nos referiremos a dicha ley como Cloud Act.

[2] H. R. 1625 – 115th Congress (2017-2018). *"Clarifying Lawful Overseas Use of Data", que se encuentra dentro de la Ley* Consolidated Appropriations Act, 2018. Disponible en idioma inglés en: http://bit.ly/2o69rE0.

Lo expuesto llamó la atención, pues la ley tiene implicancias para debatir en el orden interno norteamericano y en el ámbito internacional, como veremos seguidamente.

Lo cierto es que, en el marco de una investigación penal, el acceso por parte de las autoridades judiciales de un país determinado a datos alojados en extraña jurisdicción a través de la cooperación de la empresa proveedora de servicios en Internet, viene generando problemas jurídicos tanto para el Derecho procesal penal como para el Derecho internacional, cuyas normas de jurisdicción para la obtención de prueba están basadas en el principio de territorialidad.

Este tema también genera conflictos sobre la aplicación de normas de protección de datos vigentes en los distintos países involucrados y en las normas internacionales sobre protección de datos personales. Por ejemplo, en mayo de este año entró en vigor el Reglamento del Parlamento Europeo y del Consejo Europeo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales[3] y la Directiva del Parlamento Europeo y del Consejo Europeo, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos.[4]

Desde el ámbito de la política internacional, en supuestos en los que un Estado accede a datos alojados en extraña jurisdicción, puede inter-

[3] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, del 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) que en su artículo 48 prevé: "Artículo 48: *Transferencias o comunicaciones no autorizadas por el Derecho de la Unión*. Cualquier sentencia de un órgano jurisdiccional o decisión de una autoridad administrativa de un tercer país que exijan que un responsable o encargado del tratamiento transfiera o comunique datos personales únicamente será reconocida o ejecutable en cualquier modo si se basa en un acuerdo internacional, como un tratado de asistencia jurídica mutua, vigente entre el país tercero requirente y la Unión o un Estado miembro, sin perjuicio de otros motivos para la transferencia al amparo del presente capítulo".

[4] Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, del 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.

pretarse por parte de algunos países y organismos internacionales, como violatorio a la soberanía nacional del Estado en el que los datos informáticos están alojados[5].

Las complicaciones más frecuentes a las que se enfrentan los investigadores consisten en poder entender la inexistencia de fronteras físicas y la aceptación del desdibujado principio de territorialidad y soberanía de los Estados que surge en el marco de las investigaciones en entornos digitales.

La práctica demuestra que en este tipo de investigaciones, para lograr su eficiencia, se requiere inexorablemente acceder a información alojada físicamente en extraña jurisdicción, y sin esa información se vuelve imposible continuar con la persecución penal.

Pero además de lo señalado, esa información no solamente significa un dato fundamental para el avance de la investigación, sino que también, y en razón del carácter volátil de los datos necesarios, deviene fundamental contar con ella de manera inmediata. Hoy acudir a los mecanismos tradicionales de cooperación internacional —como el MLAT,[6] que será desarrollado posteriormente— implicaría poner en riesgo el avance de la investigación, pues los tiempos que demanda su tramitación perjudican el éxito de aquella.

En consecuencia, y ante la ineficacia de estos mecanismos tradicionales de cooperación internacional en materia penal, actualmente representa una costumbre internacional obtener los datos mediante una comunicación directa de los investigadores de un Estado determinado con las empresas del sector privado ubicada en extraña jurisdicción, en cuyos servidores están alojados físicamente los datos necesarios para un proceso penal.

En ese sentido, Salt señala: "La carencia de herramientas procesales que prevean esta nueva realidad o de canales de cooperación internacional entre países que permita la obtención de evidencia transfronteriza de

[5] El acceso transfronterizo de datos y el acceso a datos en la nube es tratado en profundidad por Marcos Salt, en su tesis "Nuevos desafíos de la evidencia digital: acceso transfronterizo y técnicas de acceso remoto a datos informáticos", Buenos Aires, Ad-Hoc, 2017, pp. 187 y ss.

[6] Tratados de Asistencia Legal Mutua. En Argentina se celebró el Tratado de Asistencia Mutua en Asuntos Penales con el Gobierno de Estados Unidos, Ley N.º 24.034, sancionada el 27 de noviembre de 1991 y promulgada 21 de diciembre del mismo año.

manera legítima y con la rapidez que la investigación requiere constituye un obstáculo tanto para la eficacia de la investigación como para la plena vigencia de las garantías no solo de los imputados de un delito, sino también de terceras personas —ISP— que pueden resultar afectadas por las distintas modalidades de acceso transfronterizo realizadas de hecho por las autoridades de los diferentes países"[7]. En consecuencia, es peligroso para las libertades individuales que un Estado acceda a datos alojados en extrañas jurisdicciones fuera de un marco que regule los principios y garantías de las personas afectadas por la intervención estatal. En este sentido, varios países se encuentran debatiendo los desafíos ya indicados y ensayando posibles respuestas y soluciones.[8]

Entendemos que la Cloud Act viene de alguna manera, más allá de la falta de debate y de las preocupaciones que causa a los organismos civiles, a iniciar un camino que requiere inexorablemente de una regulación inmediata de cooperación internacional entre países que posibilite la obtención transfronteriza de datos de manera legítima y con la rapidez que este tipo de investigaciones requiere.

2. Acuerdos de Asistencia Legal Mutua (MLAT)

Teniendo en cuenta que muchos de los proveedores de servicios de Internet tienen asiento en países extranjeros, ¿cómo solicitaremos desde la Argentina los datos de comunicaciones relacionados con un usuario que estamos investigando? La Ley N.º 24.034[9] aprobó el Tratado de Asistencia Mutua en Asuntos Penales con el Gobierno de Estados

[7] Salt, M., ob. cit. 5. p. 199.

[8] En este sentido, se pueden consultar dos propuestas elaboradas por la Comisión Europea sobre la designación de representantes de las empresas prestatarias de servicios en Internet y un reglamento sobre órdenes de entrega y conservación de pruebas electrónicas, todo ello en el marco de investigaciones penales y en relación a compañías con asiento en la Unión Europea, o que prestan servicios en ella, sin perjuicio del lugar en que alojen sus datos: "Proposal for a directive of the european parliament and of the council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings. COM/2018/226 final - 2018/0107 (COD). Strasbourg, 17.4.2018" y "Proposal for a regulation of the european parliament and of the council on European Production and Preservation Orders for electronic evidence in criminal matters. COM/2018/225 final - 2018/0108 (COD). Strasbourg, 17.4.2018".

[9] Ob. cit. 6.

Unidos, con el objeto de intentar mejorar la eficacia en las investigaciones mediante la cooperación y asistencia mutua. Este acuerdo prevé un mecanismo que aspira a lograr una comunicación más ágil a la hora de requerir información alojada en el país extranjero, aunque en la práctica esto no sucede[10].

En el marco de las investigaciones llevadas a cabo en la Fiscalía Especializada en Delitos Informáticos, hemos utilizado dicho instrumento para la solicitud de datos de contenido[11] de usuarios investigados en el marco de casos penales a ciertos proveedores del servicio de comunicaciones con asiento en Estados Unidos, previa autorización del juez en atención a las protecciones previstas en nuestra Constitución con relación a la privacidad de las comunicaciones.

El trámite debe cumplir con ciertas formalidades previstas en el tratado y los pasos a seguir son los siguientes:

1. Se dirige la solicitud al Director Nacional de Cooperación Internacional Jurídica del Ministerio de Justicia de la Nación, acompañando el oficio al fiscal y/o juez norteamericano, donde se detalla la relación entre el cliente respecto del que se solicita la información y el delito investigado[12]. De esta forma el pedido es remitido al Ministerio de Justicia para su diligenciamiento, quien luego lo remitirá a la Oficina de Asuntos Internacionales en la División Criminal del Departamento de Justicia de Estados Unidos.

2. Esta oficina realiza una revisión de la solicitud de asistencia, y en caso de considerar que esta posee toda la información y cuenta con el formato requerido, transmite el pedido a un fiscal con jurisdicción

[10] Ver artículo 1 (2) (b): "1. Las Partes Contratantes conforme a lo dispuesto en el presente tratado, se prestarán asistencia mutua, en materia de prevención, investigación y enjuiciamiento de delitos, y en los procedimientos relacionados con cuestiones penales. 2. La asistencia comprenderá: […] b) la facilitación de documentos, expedientes y elementos de prueba […]".

[11] Permiten determinar la información intercambiada por las partes que intervinieron en la comunicación.

[12] Ver artículo 4 (2): 2. La solicitud habrá de incluir lo siguiente: a) el nombre de la autoridad encargada de la investigación, del enjuiciamiento o de los procedimientos a que la solicitud se refiera; b) la descripción del asunto y la índole de la investigación, del enjuiciamiento o de los procedimientos, con mención de los delitos concretos a que el asunto se refiera; c) la descripción de las pruebas, de la información o de otro tipo de asistencia que se solicite, y d) la declaración de la finalidad para la que se solicitan las pruebas, la información u otro tipo de asistencia.

en el lugar donde la evidencia se encontraría (por ejemplo, donde se hallan las oficinas comerciales de Google o de Microsoft, en caso de requerir contenido de correos electrónicos cuyo servicio es ofrecido por esas empresas).

3. El fiscal lo remite a una corte de distrito federal para solicitar una orden de presentación u orden de registro.

4. Antes de autorizar el pedido, la corte revisará el pedido para asegurar el cumplimiento del Tratado de Asistencia Mutua y el respeto a las leyes y Constitución norteamericana.

5. En caso de que esos requisitos estén cumplimentados, se emite la orden a la empresa prestataria.

6. La respuesta de la compañía es recibida por la justicia.

7. La información suministrada es remitida a la Oficina de Asuntos Internacionales ya mencionada y al FBI. Estas oficinas estatales revisan el material con el fin verificar si la información divulgada por la empresa guarda relación con requerido por el país solicitante[13].

¿Cuánto tarda este proceso? De acuerdo con un informe realizado en Estados Unidos, todo el proceso detallado (una vez que el pedido llega a la Oficina de Asuntos Internacionales) toma alrededor de diez meses, período que se corresponde con la demora de los requerimientos realizados desde la Justicia de la Ciudad Autónoma de Buenos Aires[14]. Ello, en caso de que todas las revisiones a las que fuera sometido el pedido fuesen exitosas.

Como se advierte, el mecanismo requerido por el MLAT detallado más arriba es sumamente lento y no está a la altura del rápido desarrollo de la tecnología y su correlativa necesidad de una intervención rápida y eficaz por parte de las autoridades judiciales frente a la comisión de un delito.

[13] Mulligan, Stephen P. "Cross-Border Data Sharing Under the Cloud Act", CRS, report prepared for Members and Committees of Congress, 23 de abril de 2018, p. 14 vlta.

[14] Ver "President's Review Group on Intelligence & Communications Technologies, Liberty and Security in a Changing World: Report and Reccomendations 227", 2013.

3. Contexto legal en Estados Unidos: Ley de Privacidad de Comunicaciones Electrónicas y Ley de Comunicaciones Almacenadas

En 1986, el Congreso de Estados Unidos aprobó la Ley de Privacidad de Comunicaciones Electrónicas[15] —ECPA— que reguló el desarrollo de las nuevas tecnologías. La ley está estructurada en tres títulos: el Título I se aboca a la regulación de la interceptación en tiempo real de comunicaciones orales o electrónicas[16]. El Título II regula el acceso a comunicaciones electrónicas almacenadas y es denominada Ley de Comunicaciones Almacenadas,[17] resultando aplicable a diferentes formas de comunicación electrónica, como así también a los datos relacionados a estas: e-mails, mensajes de texto, mensajes privados, publicaciones o comentarios realizados a través de diferentes redes sociales[18]. Ofrece a los usuarios protección de la privacidad de los datos en posesión de los proveedores del servicio de comunicaciones electrónicas o de los proveedores de su almacenamiento o procesamiento remoto. Finalmente, el Título III regula el uso de dispositivos que permiten capturar información asociada a las comunicaciones, como ser números de teléfono marcados[19]. La Cloud Act enmendó en marzo de este año la Ley de Privacidad de Comunicaciones Electrónicas (ECPA), como veremos más adelante.

Por su parte, la Ley de Comunicaciones Almacenadas prevé dos componentes fundamentales como excepción a la regla general, que es la prohibición de divulgación de datos relacionados a comunicaciones electrónicas por parte de los proveedores del servicio de comunicaciones electrónicas o de los proveedores de su almacenamiento o procesamiento remoto.[20]

El primero de ellos detalla los supuestos de divulgación voluntaria de la información por parte de las empresas prestatarias de servicios en Internet, y el segundo, los mecanismos necesarios que el gobierno

[15] Electronic Communications Privacy Act. Pub. L. No. 99-508 (1986). 18 U.S.C § 2701-11.
[16] Wiretap Act 18 U.S.C § 2510-22.
[17] Stored Communications Act. SCA.18 U.S.C § 2701-11.
[18] Mulligan, S., ob. cit., p. 3.
[19] Pen Register Statute. 18 U.S.C § 3121-27.
[20] Ver artículo 18 USC § 2702 (a).

debe satisfacer para ordenar la revelación de esa información a las compañías.

En el primer caso, la ley prevé específicos supuestos en los que la revelación voluntaria de datos por parte de la empresa que presta servicios al público está permitida. La ley diferencia entre la divulgación de datos de contenido de las comunicaciones y otros datos relacionadas a las mismas.

Con relación a los datos de contenido, se prevén ocho supuestos: cuatro de ellos son de sentido común, como por ejemplo, si la persona cuyos derechos serían afectados consiente la divulgación. Entre las cuatro excepciones restantes encontramos que la empresa prestataria puede divulgar la información del cliente en caso de emergencia grave o cuando inadvertidamente descubre evidencia relacionada a un delito; por ejemplo, se encuentra específicamente prevista la situación en que la empresa advierta imágenes de pornografía infantil en la cuenta del cliente,[21] situación que da origen a muchos casos que llegan a nuestro país a través del National Center for Missing and Exploited Children (NCMEC). En consecuencia, estos supuestos constituyen las excepciones que permiten la divulgación de datos de contenido por parte de los proveedores del servicio de comunicaciones electrónicas o de los proveedores de su almacenamiento y procesamiento remoto, sin requerimiento específico previo.

En el caso de otros datos relacionados con las comunicaciones, los supuestos para la divulgación voluntaria resultan muy similares a los detallados anteriormente.[22]

El segundo componente está relacionado con los mecanismos previstos para que el gobierno ordene la revelación de datos personales, que podrían resumirse de la siguiente forma: la ley ofrece tres procedimientos según el grado de intrusión que representan respecto del tipo de dato requerido.

1. En el escalón más bajo se encuentra el requerimiento de información,[23] por ejemplo, por parte del fiscal en nombre del Gran Jurado. A través de esta solicitud, se logra obtener información básica del usuario. Este tipo de solicitud, combinada con un aviso previo al cliente, permite

[21] Ver artículo 18 USC § 2702 (b). Específicamente (b) (6) en lo referido al NCMEC.
[22] Ver artículo 18 USC § 2702 (c).
[23] En inglés denominado específicamente *subpoena*.

obtener tres categorías de información: información básica del usuario, correos electrónicos leídos que fueron almacenados, u otros archivos almacenados temporalmente, como e-mails no leídos, por más de 180 días.

2. El segundo procedimiento que se prevé es una orden de presentación emanada de una corte, con aviso previo al cliente y a través de la cual se puede obtener la misma información que con el requerimiento anterior, como así también otros datos como la historia de todos los correos electrónicos recibidos y enviados por el cliente (no así su contenido). Para este caso, el fiscal debe demostrar que cuenta con elementos que permitan razonablemente suponer que la información será relevante para la investigación penal en curso.

3. El tercero y último mecanismo previsto es la orden de registro, que resulta necesaria para poder hacerse de todos los datos e información obrante en una cuenta de correo, por ejemplo, correos no leídos almacenados por menos de 180 días y sin aviso al cliente. El estándar requerido para la orden de registro es mayor que el necesario para la orden de presentación emanada por una corte.[24]

4. El caso "Microsoft/Ireland" como precedente de la Cloud Act

El día 4 de diciembre de 2013, un juez a cargo de un Tribunal de Distrito de Nueva York emitió una orden de registro en un caso en el cual se investigaba a una persona que poseía una cuenta de correo electrónico de la empresa Microsoft Corp. La solicitud de la orden de registro se basó en el estándar de "causa probable"[25] y fue dirigida principalmente a recopilar los contenidos de todos los correos electrónicos del sospechoso, como así

[24] Ver Kerr, Orin, *Computer Crime Law*, Fourth Edition, American Casebook Series, West Academic Publishing, 2018, p. 681, y Davis, Frederick T. A U.S Prosecutor's Access to Data Stored Abroad – Are There Limits?, pp. 4 y 5. Publicado en *The International Lawyer*. Disponible en: http://bit.ly/2nh8Xuo.

[25] Aquí alude al estándar de *probable cause*. De acuerdo a la doctrina y jurisprudencia norteamericana, es un estándar sustantivo que define el nivel de sospecha necesario para poder registrar o secuestrar determinadas personas, inmuebles, cosas… La Corte norteamericana lo ha definido como "razonable de acuerdo a las circunstancias totales del caso". Livingston, Debra y otros, Criminal Procedure. Investigation and Right to Counsel, Tercera Edición, Editorial Wolters Kluwer, pp. 417-1432. El mecanismo para solicitar una orden de registro y secuestro en estos términos se encuentra en la Reglas Federales de Evidencia, Procedimiento Criminal, Artículo 41.

también otros datos relacionados a esa cuenta: datos de creación, *logs* de conexión, etcétera.

Una vez presentada la orden emitida por el magistrado, Microsoft proveyó información básica sobre su cliente junto con una moción para anular la orden respecto de los datos de contenido solicitados, basando su requerimiento en que los datos requeridos se encontraban almacenados en Dublín, Irlanda. La empresa indicó que cumplir con la orden emitida por el juez implicaría aplicar extraterritorialmente las leyes norteamericanas. El juez denegó la moción argumentando que la orden prevista en la ley, en este caso, se ejecutaba como un mero requerimiento, ya que los agentes del gobierno no debían ingresar en ningún lugar de la empresa para buscar y apoderarse de la cuenta de correo electrónico; tan solo se esperaba que la compañía suministrara la información en su posesión, independientemente de su ubicación[26].

La empresa Microsoft Corp. apeló la decisión y el Tribunal del Segundo Circuito revocó la decisión del juez de distrito con fecha del 14 de julio de 2016 y, en su decisión, el tribunal declaró que, según el texto la ley y el análisis de extraterritorialidad realizado en "Morrison v. National Australia Bank Ltd.",[27] la Ley de Almacenamiento de Comunicaciones solo tiene efectos dentro del territorio de Estados Unidos. Por lo tanto, no se podría utilizar una orden emitida por un magistrado nacional para obligar a la proveedora del servicio a divulgar los correos electrónicos almacenados en un país extranjero.

En consecuencia, el Departamento de Justicia presentó una petición para una nueva audiencia, para que el caso fuera revisado, la cual fue denegada el 24 de enero de 2017[28]. Esta decisión fue muy ajustada (cuatro jueces a favor y cuatro en contra).

La juezz Susan L. Carney —que concurrió en la denegatoria de la nueva audiencia— afirmó que la Ley de Comunicaciones Almacenadas no aplica a los correos electrónicos almacenados en el extranjero y solo tiene efectos dentro del territorio en el que fue legislada (es

[26] Microsoft Corp. v. United States (In the Matter of Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp). 829 F.3d 197 (2nd Cir. 2016).
[27] Morrison v. National Australia Bank Ltd. 561 U. S. 247 (2010).
[28] Microsoft Corp v. United States, ob. cit. 26.

decir, Estados Unidos). Argumentó que el Congreso no tenía la intención de que los procedimientos de autorización de divulgación de datos se aplicaran extraterritorialmente. Este análisis se basó en consideraciones sobre los conceptos de soberanía nacional, territorialidad y diferentes preocupaciones emanadas de los conceptos del Derecho internacional. También afirmó que el objetivo de la ley es la protección de la privacidad del usuario, y que el lugar de la protección de la privacidad es el lugar de almacenamiento de datos. En este caso, el lugar de almacenamiento de datos es Irlanda, por lo que la aplicación del estatuto sería extraterritorial. También señaló que para abordar las necesidades de cooperación entre países, el gobierno ha acordado la asistencia judicial recíproca y el cumplimiento de diferentes tratados internacionales —como los MLAT— con otros Estados soberanos[29].

Es muy interesante analizar las opiniones opuestas expresadas por los jueces José A. Cabranes, Dennis Jacobs, Reena Raggi y Christopher F. Droney[30]. Resumiremos algunos de los principales argumentos. Estos jueces indicaron que la disidencia ignoraba que Microsoft Corp. tiene en realidad acceso a la información obrante en la cuenta de correo electrónico que se encontraba alojada en Irlanda, desde suelo estadounidense y que está legalmente en posesión de ella. La decisión sostenida por los demás jueces implicaría entonces que el gobierno nunca obtendría una orden para su producción, pese a que la información se puede acceder desde suelo norteamericano, debido a que los datos se almacenan en el extranjero. De ello se sigue que esta situación brindaría amplia protección a posibles imputados de un delito. La decisión asimismo generará que los principales proveedores de servicios de Internet reduzcan su cooperación con la ley. En esta misma línea, indicaron que la disidencia omitió analizar la existencia de diferentes estructuras adoptadas por cada proveedor, consistente en que la información puede ser fragmentada y almacenada en diferentes países, o que esta pueda migrar constantemente de un servidor a otro en diferentes partes del globo, y que, a veces, la ubicación en la que los datos que se almacenan fuera de Estados Unidos

[29] Microsoft Corp v. United States, ob. cit. 26. p. 2-12.
[30] Ídem. p. 1-18.

se desconoce. También argumentaron que es la ubicación de la divulgación del proveedor lo que determinará si la Ley de Comunicaciones Almacenadas se aplica a escala nacional o extraterritorial. Dado que la divulgación y el acceso tienen lugar desde la oficina de Microsoft Corp. en Redmond, Washington, el caso demuestra una aplicación nacional del estatuto.

Además, argumentaron que la orden prevista en el artículo 2703 (a) del cuerpo legal no constituye una orden de registro tradicional, toda vez que no está dirigida a la búsqueda o secuestro de evidencia digital en el lugar, por parte de Agentes Federales. Asimismo, esta es ejecutada con relación a un individuo, que se encuentra en territorio norteamericano y sujeto a la justicia estadounidense. En consecuencia, la ejecución de la orden es una aplicación doméstica de la ley estadounidense. Justamente lo que se está solicitando es la "producción" o "presentación" de esa evidencia.

Existen varios puntos y argumentos por analizar en el presente caso, sin perjuicio de ello, nos centraremos en preguntas más generales: ¿cómo debemos proceder cuando la evidencia digital que se necesita en una investigación se almacena en un servidor extranjero? ¿Se debe considerar la evidencia en cuestión como obtenida en suelo extranjero? ¿O se puede considerar, debido a que no se necesita presencia física en el extranjero y que los datos se pueden recuperar desde el país donde se realiza la investigación, que no surgen problemas territoriales?

Como señala Frederick Davis,[31] el ejercicio de la jurisdicción ha estado tradicionalmente vinculado al territorio de un Estado. Por lo tanto, se acepta generalmente que si un Estado ejerce sus poderes jurisdiccionales en otro Estado, eso constituiría una violación de la soberanía nacional y principio de territorialidad.

Por su parte, Orin Kerr[32] indica que cuando la evidencia digital se encuentra en el exterior, el mecanismo implementado entre los Estados para obtener dicha evidencia se rige por la asistencia legal mutua. Hay dos caminos a seguir:

[31] Davis, F. ob. cit. 24. p. 7.
[32] Kerr, O., Computer Crime Law, Third Edition, West Editor, 2012, p. 752.

a) exhortos o

b) tratados de asistencia legal mutua (MLAT), acordados por varios países.

Sin embargo, como ya se ha indicado, la práctica demuestra que este canal de comunicación entre diferentes países, en cuanto a la evidencia digital, no es tan eficiente como se supone que debe ser, y para cuando el país requerido analiza el MLAT, es posible que la evidencia digital ya no exista y/o haya migrado a otro servidor, en otro país. Sin embargo, en lo que respecta a la soberanía y a las preocupaciones territoriales, estos son los pasos acordados por los países para reunir evidencias ubicadas en un país diferente del que se lleva a cabo la investigación criminal, como se señaló en la decisión del panel mayoritario en el caso "Microsoft/Ireland".

Sin embargo, a veces la información o los datos pueden almacenarse en un servidor desconocido o incluso fragmentado, lo que hace que la opción del canal MLAT no sea aplicable. En este escenario, ¿a quién se dirigiría el MLAT o el exhorto?

Este problema surgió en un caso en el que se requirieron datos de un usuario a la empresa Google, del 3 de febrero de 2017, con intervención de un juez del Distrito de Pensilvania.[33] Allí, como en el caso "Microsoft/ Ireland", se emitió una orden de registro que solicitó a Google la producción de correos electrónicos de un cliente de dicha compañía. Google respondió que la empresa había fragmentado la información en diferentes servidores, ubicados en diferentes países. Indicó además que los datos migraban automáticamente de un lugar a otro. Por lo tanto, no podía conocer exactamente la soberanía de qué país se vería implicada[34]. En consecuencia, se negó a revelar la información solicitada citando la decisión del Tribunal del Segundo Circuito en el caso "Microsoft/ Ireland". Vale la pena señalar que el acceso a toda la información podía ser habilitado por Google desde su oficina ubicada en Estados Unidos. El juez, en consecuencia, decidió obligar a Google a cumplir con la orden. En su decisión, el juez argumentó que la conducta relevante para la Ley

[33] *In re* Warrant No. 16-960-M-01 to Google en Orin Kerr, "Google must turn over foreign-stored emails pursuant to a warrant, Court rules", *The Washington Post* (February 3rd, 2017).
[34] *In re* Warrant No. 16-960-M-01 p. 26/27.

de Comunicaciones Almacenadas tendrá lugar en Estados Unidos, que no constituía una instancia de "búsqueda e incautación" fuera del país y que la invasión real de la privacidad del cliente ocurriría cuando la revelación tiene lugar, es decir, en suelo americano. La mención de este caso apunta a demostrar que encontrar una solución a esta discusión parecía una expectativa lejana y extremadamente compleja, tanto desde un punto de vista legal como político.

En este sentido, Orin Kerr[35] predijo estos escenarios poco después de la decisión del 14 de julio de 2016, cuando el tribunal del Segundo Distrito manifestó que no correspondía que Microsoft Corp. entregara los datos de contenido requeridos. El autor afirmó que no todas las estructuras de cada proveedor de servicios de Internet son iguales a las de Microsoft, y que la información puede dividirse y fragmentarse en diferentes servidores en distintos países. A veces, argumentó, la red es tan complicada en su estructura que la información solo puede ser consultada desde las oficinas de Estados Unidos.

Ahora bien, en el caso en análisis, "Microsoft/Ireland", el gobierno apeló la resolución a la Corte Suprema[36]. El 27 de febrero de 2018 se desarrollaron los argumentos orales sobre las posturas sostenidas por las partes. Todos los jueces de la corte efectuaron preguntas y discutieron los principales puntos controversiales del caso: previsiones de la Ley de Comunicaciones Almacenadas, MLAT, principio de territorialidad, entre muchos otros. Asimismo y en el marco de esa audiencia, la jueza Ginsburg y otros jueces indicaron que la respuesta podría ser legislativa[37]. Se esperaba una resolución de la corte sobre esta temática para este año; sin embargo, la modificación efectuada a la Ley de Comunicaciones Almacenadas, a través de la denominada Cloud Act, generó que la corte no

[35] Orin, Kerr, "The surprising implications of the Microsoft/Ireland warrant case", *The Washington Post* (29 de Noviembre de 2016).

[36] United States v. Microsoft Corp., 135 S. Ct. 356 (2017) (mem. granting government's petition for certiorari).

[37] Argumentos Orales de la Corte Suprema, 27 de febrero de 2018, disponible en: http://bit.ly/2o7C3wg. En este sentido la jueza Ginsburg expresó: "… If Congress takes a look at this, realizing that much time and — and innovation has occurred since 1986, it can write a statute that takes account of various interests. And it isn't just all or nothing. So wouldn't it be wiser just to say let's leave things as they are; if — if Congress wants to regulate in this brave new world, it should do it?", p. 6

tuviese necesidad de pronunciarse al respecto, ya que justamente se ofreció una solución legislativa al conflicto planteado en el caso analizado.

5. Una respuesta legislativa: la Cloud Act

El Congreso resolvió el problema planteado en el caso "Microsoft/Ireland" a través de la sanción de la Cloud Act",[38] que modificó la Ley de Privacidad de Comunicaciones Electrónicas y sus tres títulos, dentro de ellos la Ley de Comunicaciones Almacenadas debatida en el caso.

Dentro de varios cambios que la legislación efectuó, podemos resaltar dos aspectos principales. El primero, relacionado con el alcance de las órdenes emanadas por la autoridad norteamericana —tema tratado en el caso Microsoft—, y en segundo lugar y de interés para la Argentina, el problema de países extranjeros que buscan datos relacionados con comunicaciones que administran proveedores de servicio de Internet en Estados Unidos.[39]

A través de la reforma de la Cloud Act se habilita —de acuerdo con los mecanismos previstos específicamente— la divulgación de los datos en posesión de los proveedores de servicios de Internet, sin perjuicio de que dicha información se encuentre dentro o fuera de Estados Unidos[40].

Con relación al primer punto —es decir, en cuanto a las órdenes efectuadas por Estados Unidos en casos análogos a Microsoft, solicitando datos a un proveedor que los aloja en un país diferente—, la nueva ley establece un sistema para que la empresa prestataria pueda oponerse a dicho pedido por diferentes razones que deberán ser evaluadas por parte de los tribunales.

---

[38] "Clarifying Lawful Overseas Use of Data Act", parte del "Consolidated Appropiations Act", 2018, Pub. L. 115-141.

[39] Daskal, Jennifer, "Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0", *Stanford Law Review*, vol. 71, mayo de 2018, p. 11.

[40] Ver artículo 18 U.S.C § 2713 que indica bajo el título de Conservación e información obligatoria sobre comunicaciones y grabaciones, que un proveedor de servicios de comunicaciones electrónicas o de computación remota (en la nube), deberá cumplir con las obligaciones de este capítulo para preservar, conservar en seguridad o revelar el contenido de una comunicación electrónica o por cable y cualquier registro u otra información perteneciente a un cliente o suscriptor en posesión, custodia o control de dicho proveedor, independientemente de si dicha comunicación, registro u otra información se encuentra dentro o fuera de Estados Unidos.

El proveedor de servicios al que se requiere esa información dispone de catorce días para oponerse al requerimiento solo cuando todas estas condiciones se dan en el caso: *(a)* se está solicitando el contenido de las comunicaciones; *(b)* el proveedor considere razonablemente que el cliente o suscriptor no sea ciudadano de Estados Unidos o que no reside Estados Unidos; *(c)* la divulgación involucra la ley de un país que ha sido designado como un gobierno extranjero calificado; y *(d)* que la divulgación de dicha información requerida crearía un riesgo importante de que el proveedor infringiera las leyes de un gobierno extranjero calificado, concepto que será explicado más adelante[41].

Asimismo, el tribunal puede modificar o anular el contenido del requerimiento, *solo* si determina: *(a)* que la divulgación de la información requerida provocaría que el proveedor infringiera las leyes de un gobierno extranjero calificado; *(b)* considerando el conjunto de circunstancias concurrentes, el interés de la justicia determina que el proceso debe ser modificado o anulado; y *(c)* el cliente o suscriptor no es natural de Estados Unidos y no reside en Estados Unidos.

A estos fines, el tribunal tendrá en cuenta, según proceda: *(a)* los intereses de Estados Unidos, incluidos los intereses de investigación de la entidad gubernamental que solicita la información; *(b)* los intereses del gobierno extranjero calificado en prevenir cualquier divulgación de información prohibida; *(c)* la probabilidad, el alcance y la naturaleza de las sanciones que pudiese sufrir el proveedor del servicio o cualquiera de sus empleados como resultado de exigencias legales a las que pudiese estar sometido; *(d)* la ubicación y la nacionalidad del cliente cuyas comunicaciones son objeto de investigación, si se conocen, y la naturaleza y alcance de la conexión del suscriptor o del cliente con Estados Unidos, o si el proceso legal se ha iniciado a solicitud de una autoridad extranjera, la naturaleza y el alcance de la conexión del abonado o cliente con el país de dicha autoridad extranjera; *(e)* la naturaleza y el alcance de los vínculos del proveedor y su presencia en Estados Unidos ; *(f)* la importancia para la investigación de la información requerida; *(g)* la posibilidad de acceso oportuno y efectivo a la información a través de medios que cau-

[41] Ver artículo 18 U.S.C § 2703(h)(2)(A).

sarían consecuencias negativas menos serias; y *(h)* si el proceso legal ha sido iniciado en nombre de una autoridad extranjera[42].

En el segundo supuesto, con relación a gobiernos extranjeros que buscan acceso a información de comunicaciones alojada en Estados Unidos, la Cloud Act permitiría superar los problemas de ineficiencia ya apuntados con relación al MLAT en el punto 2).

Como ya se ha indicado, la ley enmendó los tres títulos de la Ley de Privacidad de Comunicaciones Electrónicas para dar respuesta a solicitudes realizadas por países extranjeros, como se explicará a continuación. Las modificaciones efectuadas permiten requerir directamente a proveedores del servicio de comunicaciones electrónicas dirigidas al público o a los proveedores de su almacenamiento o procesamiento remoto ubicados en Estados Unidos, sin pasar por los canales de los tratados de asistencia mutua:[43]

1. los datos que posean respecto de las comunicaciones de un cliente (datos de contenido y otros datos relacionados a la comunicación e información del usuario);[44]

2. interceptar o divulgar comunicaciones electrónicas;[45]

3. instalar un dispositivo de rastreo[46].

La nueva ley remueve los obstáculos y prohibiciones legales para que la empresa pueda divulgar esos datos de comunicaciones, sin que su accionar sea ilegal[47]. Para llegar a esta instancia, el país extranjero debe haber sido considerado como un "gobierno extranjero calificado". ¿Cómo se considera que un gobierno es un "gobierno extranjero calificado"? El mecanismo está detallado en el artículo 18 U.S.C § 2523, y prevé la celebración de un acuerdo bilateral con el gobierno norteamericano. Como señala Orin Kerr, el proceso es bastante complejo[48] y puede resumirse de la siguiente manera:

---

[42] Ver artículo 18 U.S.C § 2703 (h) (2) (B) y siguientes.
[43] Kerr, Orin, "Computer Crime Law. Summer 2018 Case Supplement", p. 35 vlta.
[44] Ver artículo 18 U.S.C § 2702(b) (9).
[45] Ver artículo 18 U.S.C § 2511 (j).
[46] Ver artículo 18 U.S.C § 3121 (a).
[47] Kerr, Orin, ob. cit. 43, p. 35 vlta.
[48] Ídem p. 36. Ver 18 U.S.C § 2523, donde se enumeran todos los requisitos y el mecanismo en detalle.

1. El país extranjero debe celebrar un acuerdo de asistencia legal mutua con Estados Unidos que satisfaga diversos requerimientos, entre ellos se analiza si:

a) el país extranjero posee leyes de fondo y forma y prácticas que demuestren respeto a las leyes y principios de no discriminación, protección de la privacidad y libertades civiles;

b) el país extranjero demuestra respeto por los derechos humanos;

c) el país extranjero posee suficientes mecanismos de control y transparencia con relación a la recolección y uso de datos electrónicos.

2. Una vez celebrado, el fiscal general, junto con la Secretaría de Estado, remiten certificación al Congreso indicando que el Estado extranjero ha sido calificado correctamente.

3. El Congreso puede rechazar el acuerdo: si no lo hace después de ciento ochenta días, el acuerdo entra en efecto y el gobierno extranjero se considera como "gobierno extranjero calificado" durante cinco años, período que puede renovarse en igual cantidad de años, de manera consecutiva.

4. El acuerdo celebrado debe ser "mutuo": tal como el gobierno norteamericano permite a las empresas prestatarias cumplir con los requerimientos de acuerdo con las leyes de los países requirentes y respecto de los cuales se celebró el acuerdo previsto en la ley, los gobiernos extranjeros deben permitir que aquellos proveedores que se encuentran en su país cumplan con los requerimientos legales efectuados por el gobierno de Estados Unidos.

5. El acuerdo solo autoriza al gobierno extranjero a obtener datos de extranjeros que residen fuera de Estados Unidos. Si el gobierno extranjero requiere datos de norteamericanos, residentes permanentes en dicho país y otros usuarios localizados en Estados Unidos, el gobierno extranjero deberá implementar el proceso de MLAT[49].

6. Está prohibido utilizar el acuerdo bilateral para solicitar a las empresas prestatarias desencriptar datos.[50]

Los pedidos efectuados por un país extranjero deben cumplir ciertos requerimientos y formalidades: deben referirse a una cuenta específica,

[49] Daskal, J., ob. cit. 39, p. 14.
[50] Ídem.

o persona, o dispositivo, o cualquier otro modo de identificación del usuario respecto del cual se requieren los datos; debe basarse en la necesidad de obtener información relacionada a la prevención, detección e investigación de delitos serios, el pedido debe estar razonablemente justificado en base a los hechos investigados, debe estar sujeto al control o revisión por parte de un juez o magistrado, no debe violar la libertad de expresión, no deben existir medios menos intrusivos para obtener la información requerida, entre otros. En el caso de una orden para la intercepción de una comunicación electrónica, dicha orden *(i)* debe referirse a un período fijo y limitado; *(ii)* no debe tener un plazo superior al necesario para cumplir con los fines aprobados para la orden; y *(iii)* debe emitirse únicamente si la misma información no puede obtenerse de manera razonable a través de métodos menos intrusivos. Asimismo, se prevé que el gobierno extranjero acepte un control periódico con relación al cumplimiento de los términos del acuerdo[51].

6. Críticas *versus* respaldos a la Cloud Act

Los críticos de la Cloud Act señalan que no hubo oportunidad para realizar un debate sobre sus disposiciones, pues se adjuntó a un proyecto de ley de gastos que fue aprobado por ambas cámaras del Congreso y se promulgó el 23 de marzo de 2018.

Quienes se han pronunciado en contra de la ley[52] manifestaron que dicha legislación facilitará que los países con antecedentes deficientes en materia de derechos humanos obtengan datos sensibles, otorgando mucho poder al Poder Ejecutivo sin la supervisión suficiente, obteniendo un amplio dominio sobre la privacidad digital.

Estos grupos argumentaron también que el proyecto de ley eliminó los derechos de la Cuarta Enmienda —similar al artículo 18 de nuestra Carta Magna—, contra registros e incautaciones no justificados, toda vez que el gobierno podría celebrar acuerdos de cooperación eludiendo los tribunales estadounidenses y que los usuarios titulares de los datos no serían notificados.

[51] Ver artículo 18 U.S.C § 2523.

[52] Electronic Frontier Foundation, American Civil Liberties Union, Amnistia Internacional, Human Rights Watch y Open Technology Institute.

En consecuencia, sostienen que los estándares de respeto de derechos humanos no fueron precisados específicamente, siendo vaga la explicación sobre qué prácticas excluirían a un determinado país de la posibilidad de celebrar los acuerdos previstos en la Cloud Act. Algunos de estos grupos fundamentan su oposición en que las empresas prestatarias podrían no ser rigurosas al revisar las solicitudes de ciudadanos de otros países almacenadas en servidores en Estados Unidos, permitiendo así la obtención inapropiada de esos datos.

Es claro que, desde el ámbito de la política internacional, también existen preocupaciones. En este orden, se señaló: "Escondido en el proyecto de ley general de gastos, hay una disposición que permite a Trump, y a cualquier futuro presidente, compartir correos electrónicos privados de los estadounidenses y otra información con los países que a él personalmente le gustan. Eso significa que puede llegar a acuerdos con Rusia o Turquía, con una participación casi nula en el Congreso y sin la supervisión de los tribunales estadounidenses"[53].

Por su parte, la Comisión Europea había presentado un informe en su calidad de *amicus curiae* en el caso de Microsoft, en el que si bien no apoyaba específicamente a ninguna de las partes del caso, defendió el principio de territorialidad bajo el Derecho internacional público, de la siguiente manera: "Desde la perspectiva de la Unión Europea y del Derecho internacional público, cuando una autoridad pública exige que una empresa establecida en su propia jurisdicción produzca datos electrónicos almacenados en un servidor en extraña jurisdicción, los principios de territorialidad y cortesía en el Derecho internacional público están comprometidos, y los intereses y las leyes de esa jurisdicción extranjera deben tenerse en cuenta"[54].

La Cloud Act tuvo el apoyo del Departamento de Justicia y de las principales compañías de tecnología como Microsoft, Apple y Google. Por su parte, Microsoft manifestó que dicha ley representa un marco legal moderno, y alentó al gobierno a actualizar estos acuerdos sobre los datos con otros países: "Damos la bienvenida a la decisión de la Corte

[53] Senador Ron Wyden (D-Ore).
[54] *Amicus curiae* Unión Europea en el caso US *versus* Microsoft.

Suprema […] a la luz de la entrada en vigor de la Cloud Act. Nuestro objetivo siempre ha sido una nueva ley y acuerdos internacionales con fuertes protecciones de privacidad que gobiernen cómo recolectar evidencia digital a través de las fronteras, a la luz de la aplicación de la ley".[55]

7. Conclusiones

Como hemos visto, de acuerdo con los enfoques tradicionales para reunir pruebas de otro país, deberían implementarse los canales diplomáticos. Sin embargo, esta parece ser una respuesta extraña cuando la información necesaria se encuentra en la computadora de los empleados de la empresa proveedora del servicio de Internet, en una oficina ubicada en Estados Unidos, a solo un clic de distancia. Esto demuestra la necesidad de repensar los conceptos de soberanía nacional y territorialidad tradicionales. Sin embargo, debe tenerse en cuenta que los diferentes países tienen diferentes leyes con respecto al almacenamiento y la privacidad de los datos personales.

Esta discusión también se está llevando a cabo en la comunidad internacional, donde se implementaron diferentes mecanismos para tratar de mitigar estos inconvenientes, ninguno de los cuales resultó ser tan eficiente como era necesario.

Como podemos ver, la tecnología impone nuevos desafíos a los conceptos de soberanía y territorialidad. Estas ideas nacieron en un mundo físico, en un período en el que los medios electrónicos de comunicación y la revolución de la tecnología estaban lejos de ser realidad.

Estos conceptos son difíciles de conciliar con el hecho de que Internet no tiene límites ni fronteras. No hay consenso sobre la respuesta política y legal correcta a estos fenómenos. Mientras tanto, las investigaciones criminales están en riesgo, ya que a veces la información requerida se almacena en el exterior.

El caso "Microsoft/Ireland" ha sido evidencia dqe los desafíos de esta nueva realidad y la sanción de la Cloud Act" una aproximación a una posible solución, en la incesante búsqueda de un equilibrio entre la necesidad de la persecución penal y la protección de datos personales y la privacidad.

[55] Declaraciones de Brad Smith, presidente de Microsoft.

De "Claps" a "Kosten": una correcta evolución sobre la responsabilidad de las plataformas de comercio electrónico

por Rodolfo Christophersen

Resumen: En este trabajo se podrá encontrar una pequeña síntesis de cómo ha ido evolucionando la jurisprudencia argentina relativa a la responsabilidad de las plataformas de comercio electrónico, desde sus inicios, donde se aplicaba (y aún se sigue aplicando) un factor de atribución de la responsabilidad solidario y objetivo por la aplicación irrestricta del artículo 40 de la Ley Nacional de Defensa del Consumidor y la teoría del beneficio y riesgo económico empresario, hasta la actualidad, donde algunos de los magistrados (tanto de primera como de segunda instancia) han comenzado a resolver sus casos haciendo un análisis profundo de la jurisprudencia, doctrina y legislación extranjera, aplicando un factor de atribución de la responsabilidad subjetiva y comprendiendo que la temática en cuestión no es una temática sencilla que se puede resolver mediante la aplicación de institutos del derecho que no tienen en consideración las particularidades de los modelos de negocio de las mencionadas plataformas de comercio electrónico.

Palabras clave: consumidor – defensa del consumidor – Internet – comercio electrónico – responsabilidad civil – rol activo – interpretación judicial.

Summary: In this paper, you will find a small synthesis of the evolution in the jurisprudence related with the responsibility of the e-commerce platforms. You will find how the jurisprudence in Argentine has been evolving from the unrestricted application of a strict liability institute to the application of the active roll concept, which has originated in the European Community in an important case (L'Oréal vs. eBay) with the intervention of the European High Court of Justice.

Keywords: consumer – consumer protection – Internet – e-commerce – tort law – active role – legal interpretation.

1. Introducción

Teniendo en cuenta los vaivenes que hemos sufrido en estos últimos años, y siendo que la temática de la responsabilidad de las plataformas de comercio electrónico es una temática novedosa y por demás interesante para nuestro Derecho argentino, me he tomado el trabajo de escribir este artículo a través del cual intentaré hacer un pequeño análisis de cuál ha sido la evolución de los precedentes jurisprudenciales más relevantes que se han dictado en la materia analizando en cada uno de ellos cuales han sido los argumentos jurídicos más relevantes que se han ido invocado para definir la suerte de las mencionadas plataformas de comercio electrónico.

2. Los primeros pasos: un camino con algunos altibajos

Este camino comienza con el precedente jurisprudencial dictado por la Cámara Nacional de Apelaciones en lo Civil, Sala K, el 5 de octubre de 2012, en los autos caratulados "Claps, Enrique Martin y otro c/ Mercado Libre S. A. s/ daños y perjuicios"[1].

En dicho precedente la cámara analizó la responsabilidad que le hubiera correspondido a una plataforma de comercio electrónico —por el caso, Mercado Libre— en una operación de comercio electrónico celebrada entre un usuario que había adquirido dos entradas para que sus dos hermanos pudieran asistir a un espectáculo público y un usuario vendedor que entregó dicho par de entradas que habían sido denunciadas como robadas por el agente encargado de venderlas.

En un precedente muy poco analizado y sin mayores argumentos jurídicos que la aplicación exorbitante de un factor de atribución de responsabilidad objetiva por la remisión irrestricta al artículo 40 de la Ley Nacional de Defensa del Consumidor y la teoría del riesgo y el benéfico económico empresario, la cámara entendió que Mercado Libre debía ser considerada responsable por los incumplimientos de los usuarios que ofrecen para la venta productos que están fuera de su esfera de control.

[1] CNCivil, Sala K, *in re* "Claps, Enrique Martin y otro c. Mercado Libre S.A. s/daños y perjuicios", del 5/10/2012.

Creo que es importante destacar que este fue el primer precedente jurisprudencial que se dictó sobre la responsabilidad de las plataformas de comercio electrónico, y como veremos a continuación, entiendo que dada la importancia de la cita ante la cual estaban llamados los miembros de la Sala K de la Cámara Nacional en lo Civil desaprovecharon una gran oportunidad para hacer un análisis profundo y mucho más concienzudo sobre la temática en cuestión.

En efecto, creo que este precedente fue tomado por los miembros de la Sala K de la Cámara de Apelaciones en lo Civil como un caso que no iba a tener mayor trascendencia, en tanto se puede advertir con la simple lectura de la sentencia de marras que ninguno de los camaristas analizó siquiera cómo funcionaba el sitio web de la demandada y/o cuál había sido la jurisprudencia y legislación extranjera que existía hasta ese momento.

Por el contrario, como dijimos anteriormente, los camaristas recurrieron a la aplicación lineal e irrestricta de argumentos tradicionales que poco tenían que ver con cómo se habían presentado los hechos del caso en particular.

Ahora bien, teniendo en cuenta ello, resulta importante remarcar que las consecuencias del precedente "Claps" lejos han quedado circunscriptas al caso particular bajo análisis. Es que una vez que la Sala K emitió el precedente en cuestión, este comenzó a ser replicado de manera íntegra y sin mayores reparos por los diferentes juzgadores de otros casos que las plataformas de comercio electrónico tenían abiertos hasta ese momento; podemos hacer mención de los precedentes: "Ferreiro Pablo Alberto",[2] resuelto el pasado 15 de septiembre de 2016 por la Sala Tercera de la Cámara en lo Civil y Comercial de la Provincia de Jujuy; "Hidalgo María Argentina",[3] resuelto el pasado 7 de octubre de 2016 por la Cámara de Apelaciones en lo Civil, Comercial y Minería de la Tercera Circunscripción Judicial de la Ciudad de San Carlos de Bariloche, Provincia de Río

[2] CCivil y Comercial, Jujuy, Sala III, *in re* "Acción emergente de la ley del consumidor: Ferreiro, Pablo Alberto c. Mercado Libre S.R.L.", del 15/9/2016.

[3] CACivil, Comercial y Minería de la Tercera Circunscripción Judicial, *in re* "Hidalgo, María Argentina c/ Peinado, Matías y Mercado Libre s/ compra inexistente", expte. 010836-dci-2013 s/ apelación (cc), del 7/10/2016.

Negro; y "Grifasi Carolina Nora",[4] resuelto el pasado 29 de diciembre de 2016 por la Cámara Cuarta de Apelaciones en lo Civil y Comercial de Córdoba, entre muchas otras resoluciones administrativas más que aún se encuentran bajo revisión de la instancia judicial.

En este último precedente la cámara interviniente rechazó un recurso de apelación interpuesto por la firma Mercado Libre contra una resolución sancionatoria que había impuesto la Dirección de Defensa del Consumidor y Lealtad Comercial de la Provincia de Córdoba por haber considerado que la mencionada plataforma había infringido la Ley Nacional de Defensa del Consumidor (artículos 4, 9, 11, 13 y 34) al permitir que un usuario vendedor entregara un par de zapatillas usadas cuando en la publicación que había diseñado el propio usuario vendedor había indicado que las mismas eran nuevas, y lo peor de todo es que para argumentar a esa sorprendente e inexplicable conclusión la cámara tan solo se limitó a citar textual e íntegramente el precedente origen de este artículo, es decir, "Claps".

Sin embargo, no todo han sido malas noticias para una industria que tiene como misión "promover y desarrollar la economía digital para contribuir al desarrollo social y económico de la Argentina", ya que, como veremos a continuación, al menos cierto sector de la justicia ha comenzado a tomar el tema de una manera mucho más seria, demostrando un alto grado de análisis, investigación y comprensión de la complejidad involucrada en el rol que les corresponde a las plataformas de comercio electrónico en particular.

3. Los últimos primeros pasos: un poco de luz al final del camino

En efecto, como se dijo, existen varios juzgadores que se han tomado el tiempo suficiente para estudiar una temática por demás novedosa para nuestro Derecho argentino al emitir precedentes que tienen una gran calidad técnica en cuanto a los argumentos invocados para fundamentar su decisión.

[4] Cámara 4.ª de Apelaciones en lo Civil y Comercial de Córdoba, *in re*, "Mercado Libre S.R.L. c. Dirección de Defensa del Consumidor y Lealtad Comercial s/ rec. apel. c/ decisiones autoridad adm. o pers. jurídica púb. no estatal (civil)", del 29/12/2016 (no firme).

En esa línea argumental podemos mencionar al precedente de "Nike International Ltd c/ Compañía de Medios Digitales CMD SA s/ cese de uso de marcas",[5] dictado por la Sala III de la Cámara de Apelaciones en lo Civil y Comercial Federal el 21 de mayo de 2015. En dicho precedente la cámara analizó el grado de responsabilidad que le correspondía aplicar a una plataforma de comercio electrónico —por el caso, MasOportunidades— al permitir que terceras personas publicaran para su venta productos que estaban en evidente infracción a los derechos de propiedad intelectual de su titular, por el caso Nike.

Para ello, y en tanto que los integrantes de la Sala III de la Cámara Nacional de Apelaciones en lo Civil y Comercial Federal reconocieron la dificultad que presentaba la temática que les había tocado resolver, muy acertadamente lo primero que hicieron fue estudiar el tema en cuestión analizando para ello no solo el funcionamiento de la plataforma de la demandada, sino también haciendo una ponderación profunda de la jurisprudencia y legislación extranjera que existía en la materia hasta ese momento.

Así las cosas, y solo luego de haber finalizado con el mencionado trabajo investigativo, los camaristas concluyeron que para resolver el *thema decidendum* resultaba determinante "saber si el sitio 'masoportunidades' es tan solo un intermediario que solo almacena datos de los bienes o servicios que serán objeto de las operaciones de compraventa llevadas a cabo en su plataforma o si, por el contrario, ejerce un rol activo, participando de dichas operaciones y potenciándolas publicidad mediante. La diferencia es fundamental porque el papel activo de tener conocimiento y control de los datos que almacena está en directa relación con la capacidad de evitar el uso indebido y con la responsabilidad por los daños producidos por la violación al derecho marcario".[6]

Y bajo esa línea argumental fue que la Cámara entendió que "la demandada ejercía un rol activo en las operaciones llevadas a cabo en su sitio toda vez que brindaba a sus clientes la posibilidad de potenciar las ofertas de venta y/o promoverlas mediante el abono de un plus, lo que indudablemente le daba la posibilidad cierta de acceder a un mejor control de los

[5] CNFedCivyCom, Sala III, *in re*: "Nike International Ltd c. Compañía de Medios Digitales CMD SA s/ cese de uso de marcas", del 21/5/2015.
[6] Ver párrafo 17 del considerando V de los autos antes citados.

datos", y por lo tanto debía responder subjetivamente por los daños ocasionados a Nike en tanto se había logrado acreditar que en el sitio web de la demandada "se ofrecían en venta 'réplicas', 'imitaciones', 'falsificaciones', lo que significa que no se trata de productos originales".[7]

Pues bien, fácil resultará advertir la diferencia en cómo se encaró la resolución de este precedente en comparación con el precedente dictado por la Sala K de la Cámara Nacional de Apelaciones en lo Civil. Es que a simple vista uno puede advertir una inmensa diferencia en cuanto al grado de análisis que se hizo en uno y otro caso. En uno se hizo una aplicación lineal e irrestricta de argumentos tradicionales que poco tenían que ver con cómo se habían presentado los hechos del caso en particular, mientras que en el caso bajo análisis la Sala III de la Cámara Nacional de Apelaciones en lo Civil y Comercial Federal trajo para su análisis un concepto totalmente novedoso para el Derecho argentino: el concepto del rol activo.

Con la aparición de este precedente, personalmente entiendo que ha cambiado el escenario respecto a cómo debe evaluar el grado de responsabilidad que les cabe aplicar a las plataformas de comercio electrónico, ya sea por los daños ocasionados por el contenido que alojan en sus sitios web como por los incumplimientos que pudieran llegar a ocasionar sus usuarios vendedores. Es que a partir de este precedente —aunque así debió haber sido desde el caso "Claps"— la discusión debería comenzar a pasar por identificar cuál ha sido el grado de participación que pudo haber tenido la plataforma de comercio electrónico en cada operación de comercio electrónico en particular. Es decir, se debería definir si efectivamente la plataforma en cuestión tuvo un rol activo o meramente pasivo o neutral, con todo lo que ello implica.

Así fue cómo lo entendió la Sala D de la Cámara Nacional de Apelaciones en lo Comercial al resolver el precedente caratulado "Kosten, Esteban c. Mercado Libre SRL s/ ordinario"[8] el 22 de marzo de 2018.

En efecto, en dicho precedente fue el propio vocal preopinante, el doctor Heredia, quien advirtió que si bien el actor había planteado "agravios que, en sustancia, pretenden que las cuestiones implicadas se resuelvan a base de una aplicación genérica de principios o reglas vinculadas a

[7] Ver párrafo 20 del considerando V de los autos antes citados.
[8] CNComercial, Sala D, *in re*: "Kosten, Esteban c. Mercado Libre SRL s/ ordinario", del 22/3/2018.

cuáles son los derechos del consumidor y las obligaciones del proveedor, la asimetría entre ambos, la omisión informativa en la que había incurrido la demandada y el valor que la confianza tiene en el comercio electrónico, entre otros", dada "la problemática que plantea el *sub lite* [el *thema decidendum* era] bastante más complejo que ello".[9] Por lo que luego de hacer un minucioso análisis de la legislación,[10] jurisprudencia[11] y doctrina[12] extranjera, el mencionado camarista indicó que el *thema decidendum* debía ser resuelto bajo las siguientes conclusiones:

(i) "puede hablarse de una exención de responsabilidad del operador de un mercado electrónico de ventas o subastas on line cuando no ha desempeñado un papel activo que le permita adquirir conocimiento o control de los datos almacenados, es decir, cuando ha sido un 'mero canal' limitándose a proporcionar un foro para una transacción entre un comprador y un vendedor".

(ii) "tal general exención se funda en la circunstancia de que no es posible responsabilizar al operador cuando actúa efectivamente como un mero intermediario, es decir, adoptando entre los destinatarios del servicio (comprador y vendedor) una posición neutra, meramente técnica, automática y pasiva, lo que impide que tenga conocimiento y control de la información almacenada".

(iii) "de tal suerte, el mero hecho de que el operador de un mercado electrónico almacene en su servidor ofertas de venta, determine las con-

[9] Ver primer párrafo del considerando 3.

[10] La Directiva 2000/31/CE del Parlamento Europeo y del Consejo, del 8/6/2000, relativa a "Determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior", haciendo especial hincapié en los artículos 14 y 15 de la mencionada Directiva.

[11] TJCE, 12/7/2011, "L'Oréal SA, Lancôme parfums et beauté & Cie SNC, Laboratoire Garnier & Cie, L'Oréal (UK) Ltd. c. eBay International AG", apartado 109; "Tyffany Inc. c. eBay Inc.", 576 F. Supp., 2d. 463, 469 S.D.N.Y. 2008; Bruxelles, Tribunal de Commerce, 7ème Chambre, Salle B, 31/07/2008, "Lancôme Parfums et Beauté & Cie c. eBay International AG, eBay Europe s.a.r.l., et s.p.r.l. eBay Belgium"; Cour de Cassation, Chambre commerciale, financière et économique, 3/5/2012, "eBay c. Louis Vuitton Malletier"; Tribunal de Grande Instance de Troyes, Chambre Civile, 4/6/2008, "Hermès International c. Madame Cindy F., SA eBay France et eBay International"; Tribunal de Commerce de Paris 1er., Chambre B, 30/6/2008, "Louis Vuitton Malletier c. eBay Inc., eBay International AG".

[12] Cavanillas Mugica, Santiago, *Responsabilidades de los proveedores de información en Internet*, Editorial Comares, Granada, 2007, p. 158; Peguera Poch, Miguel, *La exclusión de responsabilidad de los intermediarios en internet*, Editorial Comares, Granada, 2007, p. 322.

diciones de su servicio, sea remunerado por el mismo y dé información general a sus clientes no puede implicar que se le excluya de las exenciones de responsabilidad previstas por la Directiva 2000/31/CE".

(iv) a contrario sensu, "ninguna exención de responsabilidad puede aprobarse cuando el operador del mercado electrónico prestó un papel activo que le permitió adquirir conocimiento o control de los datos almacenados […] Tampoco si ha recibido una orden judicial que lo colocaba en situación de ejercer una 'vigilancia activa' o prestó una asistencia consistente, en particular, en optimizar la presentación de las ofertas de venta en cuestión o en promover tales ofertas".

Personalmente celebro el dictado de este precedente, no simplemente porque entiendo que ha sido la manera correcta de resolver el fondo de la cuestión, sino porque se ha tratado de una gran pieza jurídica que ha marcado el camino para los próximos precedentes que se dicten en la materia. Sobre todo, teniendo en cuenta que el mismo está en perfecta sintonía con la doctrina que surgió del *leading case* "Rodríguez María Belén c/ Google Inc. s/ Daños y Prejuicios",[13] resuelto por la Corte Suprema de Justicia de la Nación el 28 de octubre de 2014, donde se resolvió que "la inexistencia de una obligación general de vigilar le sigue —como lógico corolario— la inexistencia de responsabilidad", por lo que "la pretensión de aplicar responsabilidad 'objetiva' en este tema, es de una llamativa insustancialidad" ya que "si a la vera de un camino se desarrolla una actividad ilícita —que, por hipótesis, debe ser condenada— no por eso puede sancionarse al responsable de la ruta que permite acceder al lugar, con el peregrino argumento de que hizo más fácil la llegada a aquel"[14].

4. Conclusiones

En suma, la aparición de precedentes como los analizados en el punto anterior no son más que la confirmación de una línea jurisprudencial bien sofisticada que esperamos se vaya consolidando a lo largo del tiem-

[13] CSJN, *in re*: "Rodríguez María Belén c/ Google Inc. s/ Daños y Prejuicios", del 28/10/2014. Criterio confirmado bajo la nueva composición de la corte en el caso "Gimbutas, Carolina V. c. Google Inc. s/ daños y perjuicios", del 12/9/2017.

[14] Ver considerando 16 de los autos antes referenciados.

po y que con suerte servirán como un impulso para lograr un cambio en el eje de la discusión, virándola desde la aplicación irrestricta, infundada e irresponsable del artículo 40 de la Ley Nacional de Defensa del Consumidor y la teoría del riesgo y el benéfico económico empresario (teoría desechada expresamente por los precedentes extranjeros mencionados por la jurisprudencia extranjera invocada en los precedentes bajo análisis), hacia la definición del concepto del rol activo y sus alcances para cada plataforma de comercio electrónico en particular.

Si ello llegase a ocurrir, auguro el advenimiento de una idea de justicia que poco a poco irá abandonando las posturas tradicionalistas que han ido en detrimento de la innovación, del comercio electrónico y de una industria que día a día genera miles de nuevas oportunidades para todos los argentinos por igual.

Historia de NIC Argentina en el marco de la evolución de Internet en el país

por Julián Dunayevich, Gabriela Ramírez, Camila Trentadue, Daniel Franca y Tamara Zylbersztejn

Resumen: para entender cómo Internet fue propagándose en nuestro país y, en este contexto, cómo nació NIC Argentina y fue creciendo tanto en su función como administrador del dominio de nivel superior ".ar" como en objetivos, es necesario revisitar el devenir histórico. Los hitos que en este trabajo se resaltan no deben ser leídos como una concatenación de avances tecnológicos, sino como la reconstrucción de un camino que marcaba un modelo de trabajo colaborativo y participativo impulsado por sectores académicos y técnicos y que, paulatinamente, habilitó la incorporación de actores de las áreas más diversas, para así dar lugar, luego de un proceso de maduración, a la consolidación de instituciones en el ámbito nacional y regional como NIC Argentina que comenzarían a administrar los recursos de Internet.

Palabras clave: Internet, informática, redes, NIC Argentina.

Abstract: to understand how Internet has spread across our country and, in this context, how NIC Argentina was born and grew as administrator of the ".ar" Top Level Domain, it's necessary to revisit the historical evolution. The milestones highlighted in this work should not be read as a concatenation of technological advances, but rather as the reconstruction of a road that marked a collaborative and participative work model. A work model driven by academic and technical sectors that, gradually, enabled the incorporation of actors of the most diverse areas in order to consolidate the birth of national and regional institutions that, like NIC Argentina, would begin to manage Internet resources.

Keywords: Internet, it, networks, nic argentina.

1. Introducción

Entender la historia de Internet requiere un recorrido del pasado que nos ayude a comprender el devenir de los acontecimientos y, al mismo tiempo, pensar en el futuro y en cómo podría evolucionar. Conocer las experiencias que vivieron los pioneros, tanto sus dudas y aciertos como los desafíos que afrontaron y las discusiones que superaron, nos da la posibilidad de reflexionar de una manera crítica la trayectoria tecnológica que vivió nuestro país.

En la siguiente investigación nos proponemos recuperar y analizar la historia de NIC Argentina a partir de un exhaustivo recorrido del devenir histórico de Internet, particularmente en el contexto argentino. Tenemos como objetivo aprehender y comprender cómo se gestó un modelo que comenzó impulsado por sectores académicos y técnicos y, paulatinamente, habilitó la incorporación de actores de las áreas más diversas.

En este proceso resaltaremos la importancia que la institución tiene no sólo como registro sino también como administrador de una infraestructura crítica clave. Además, cómo NIC Argentina, encargado de administrar este recurso de Internet, también fue creciendo en metas y objetivos para transformarse en un actor integrante de las diversas discusiones actuales, principalmente técnicas y políticas, y que traspasan las barreras del universo técnico.

2. Antecedentes: la computación en Argentina como cuna de científicos

Para entender la historia de NIC Argentina[1] en el marco de los orígenes de Internet en el país, es necesario conocer el camino del desarrollo de la informática a escala nacional. Este es un proceso que implica ir tras las huellas de un grupo de trabajo de investigadores que desde la Facultad

[1] Network Information Center Argentina, en español, Centro de Información de la Red para Argentina. Organización dependiente de la Secretaría Legal y Técnica de la Presidencia de la Nación Argentina, bajo la órbita de la Dirección Nacional de Registro de Dominios de Internet, responsable de administrar el dominio de nivel superior ".ar", el registro de nombres de dominio y asegurar el funcionamiento del DNS (Sistema de Nombres de Dominio). Como representante de la comunidad técnica, es integrante del Ecosistema de Internet y participa activamente en los debates sobre Gobernanza de Internet.

de Ciencias Exactas y Naturales (FCEyN) de la Universidad de Buenos Aires (UBA) de Argentina, y a fuerza de acaloradas discusiones pero con una indiscutible dedicación, pasión y voluntad, generaron el escenario propicio para que Argentina pudiera conectarse a Internet.

La incorporación de Manuel Sadosky al Departamento de Matemática de la Universidad de Buenos Aires de estudios puede ser tomada como uno de los puntos de partida para la formalización de la carrera de Ciencias de la Computación en el ámbito académico nacional. Primero, desde su rol docente, y luego como vicedecano del doctor Rolando García,[2] Sadosky durante los primeros años de la década de 1960 impulsó la creación del Instituto de Cálculo,[3] dentro del ámbito de la UBA, e insistió con la adquisición de la primera computadora científica de la Argentina entre una de las diecinueve Mercury que produjo Ferranti, empresa oriunda de Manchester:[4] "Clementina".

La madurez de las disciplinas vinculadas a la computación todavía marcaba como secundario el rol de los programadores en el mundo científico. Cuando por fin en 1963 se creó la carrera de Computación Científica[5] de la UBA —primera de su tipo en el país y en América Latina—, todavía había una intencionalidad pragmática de formar profesionales que pudieran asistir a científicos y usuarios en el uso del nuevo dispositivo de cálculo. Con cuatro años de duración, y como parte del Departamento de Matemática, la carrera empezó a generar un círculo de profesionales que permitieron al Instituto de Cálculo realizar grandes aportes en investigaciones de la misma facultad y de otras instituciones de gestión pública y privada.

Clementina fue muy utilizada en esos primeros años para los proyectos científicos impulsados desde diversas instituciones. De hecho, los ingresos por trabajos y servicios a terceros constituyeron una porción importante del presupuesto del Instituto de Cálculo,[6] vislumbrando ya

[2] Decano de la Facultad de Ciencias Exactas y Vicepresidente fundador del Conicet.
[3] Resolución 1662 de la Facultad de Ciencias Exactas y Naturales de la Universidad de Buenos Aires. Buenos Aires, 27 de noviembre de 1957.
[4] Swann, B. "The Ferranti Computer Department", unpublished notes, 1975.
[5] Blanco, E. "50 años de la carrera de computador científico, en la UBA", Blog Portinos, 2013 [http://bit.ly/2naStEc].
[6] Czemerinski H. & P. M. Jacovkis. "La llegada de la computación a la Universidad de Buenos

en aquel entonces una naciente interrelación entre diferentes actores en pos de un beneficio mutuo.

El golpe de Estado de 1966 provocó heridas profundas que trascienden hasta la actualidad, ya que las universidades no sólo fueron intervenidas sino que también fueron escenario de violentas intervenciones policiales, en las cuales estudiantes y profesores fueron brutalmente golpeados, heridos y perseguidos. Jorge Aguirre, en la publicación *Panorama de la historia de la Computación Académica en la Argentina*,[7] afirma que esta situación trajo como principal consecuencia la renuncia masiva de numerosos docentes y el exilio obligado de cientos de científicos. Este contexto marcó un retroceso en el desarrollo de la disciplina, el cual relegó al país con relación a aquellos que estaban a la vanguardia. Hasta principios de la década de 1980, diferentes proyectos científicos fueron interrumpidos. Sin embargo, creció el parque de equipos de computación y se intensificó la demanda profesional en este campo laboral.

Paralelamente, en Estados Unidos en 1969, la Agencia de Proyectos de Investigación Avanzados (ARPA) aprobaba la primera partida presupuestaria para construir la red de computadoras que sería conocida como Advanced Research Projects Agency Network, es decir, la Red de la Agencia de Proyectos de Investigación Avanzada (ARPANET). Si bien tanto el emprendimiento como su financiamiento nacieron en el marco del Departamento de Defensa, esta iniciativa impulsaba un modelo que trascendía lo gubernamental, y el sector académico fue el principal promotor de esta red[8] que años más tarde llevaría al nacimiento de Internet.

Este escenario permite marcar el contraste que separaba a las ciencias de la computación de Estados Unidos y Argentina: al finalizar la década de 1960, luego del esfuerzo colaborativo, ARPANET se puso en marcha, pero la informática nacional, relegada al mundo académico, ya padecía un abandono que tardaría más de una década en sanearse. Sin embargo, aún ante este lúgubre panorama, la división electrónica de la Fábrica

Aires", *Revista Iberoamericana de Ciencia Tecnología y Sociedad*, vol. 6., N.º 18, Ciudad Autónoma de Buenos Aires, agosto de 2011.

[7] Aguirre, J. "Panorama de la historia de la Computación Académica en la Argentina", *Historia de la Informática en Latinoamérica y el Caribe: Investigaciones y Testimonios*, Río Cuarto, Universidad Nacional de Río Cuarto, 2009.

[8] Ferreyra, G. *Internet paso a paso: hacia la autopista de la información*, México, Alfa Omega, 1996.

Argentina de Telas Engomadas (FATE), de capitales nacionales, desplazó en el mercado argentino a la empresa italiana Olivetti en el desarrollo y la comercialización de calculadoras electrónicas con un alto nivel de integración de componentes.

3. El retorno de la democracia y el impulso a la innovación

El retorno a la democracia en Argentina en 1983 comenzó a dar un nuevo empuje a la informática en el país, generó un creciente interés por la investigación y se concentró de manera particular en el estudio de la construcción de redes, las cuales ayudarían a mejorar la comunicación de datos entre los diferentes centros académicos nacionales e internacionales.

En 1983, con la caída de la dictadura cívico-militar, autodenominada Proceso de Reorganización Nacional, se inició una etapa de necesaria renovación y, en paralelo, numerosos científicos comenzaron su retorno al país, luego de años en el exilio. Una nueva licenciatura en Ciencias de la Computación hizo su lugar en la Facultad de Ciencias Exactas y Naturales de la Universidad de Buenos Aires. Dotada de una jerarquía y autonomía añoradas por su antecesora, fue un importante primer paso. Ese mismo año, la Empresa Nacional de Telecomunicaciones (ENTel) inició el proyecto ARPAC,[9] la Red Argentina de Teleconmutación de Paquetes. Fue la primera red nacional de datos cuyo objetivo principal fue brindar el servicio de transmisión de datos a grandes empresas utilizando el protocolo X.25[10]. Este protocolo era un estándar fundamentalmente utilizado en Europa.

A fines de 1983, Gregorio Klimovsky, decano normalizador de la FCEyN (UBA), designó a Hugo Scolnik como director del Departamento de Computación. Alrededor de él se nuclearon especialistas, estudian-

[9] Amodio, J. "Los primeros pasos", Internet Argentina, Historia y evolución (blog), 2010 [http://bit.ly/2oDM8Br].

[10] X.25 es una norma de red de datos pública que el CCITT (Comité Consultivo Internacional Telegráfico y Telefónico, un organismo de la Unión Internacional de Telecomunicaciones) recomendó en 1976 por primera vez, hasta que en 1985 se estableció el estándar definitivo. La norma se constituye como una interfaz entre redes de conmutación de paquetes y dispositivos de usuarios que operan en este tipo de redes.

tes, graduados y profesores como Mauricio Fernández, Jorge Amodio, Carlos Mendioroz, Nicolás Baumgarten y Julián Dunayevich,[11] quienes empezaron a impulsar en el país la investigación y el desarrollo de redes.

Pero este nicho universitario ya no transitaba sólo el camino de la informática. Años atrás Oscar Varsavsky postulaba la construcción no de una universidad ideal, aislada de la sociedad, sino de aquella que entre en relación dialéctica con esa sociedad, buscando la transformación de ambas[12]. Esta idea recorría los pasillos de la Facultad de Ciencias Exactas, donde el objetivo era desarrollar la ciencia informática y otorgarle un estatus propio. Así, progresivamente comenzaron a surgir colaboraciones con diferentes instituciones que encontraron en este espacio un lugar propicio para la participación.

En 1985 Fate Electrónica empezó un proceso de cooperación recíproca con la facultad a través de la donación de equipamiento[13]. Ese mismo año Julián Dunayevich ingresó como becario en esta empresa para profundizar el uso de UNIX, especialmente con relación a la facilidad de los componentes de comunicaciones[14]. Allí comenzó a organizar, por un lado, el laboratorio de redes, y por otro, un curso de X.25 junto a Juan Carlos Angió, primer egresado de la carrera de Computador Científico e integrante del staff de la empresa. Tal como relata Julián Dunayevich en su testimonio:

> La historia de X.25 fue muy importante porque a ese curso invité a participar a Mauricio Fernández, a Jorge Amodio y a Carlos Mendioroz, entre otros. Todos recibimos el curso que dictó Juan Carlos, y de ahí empezamos a armar un grupito al que le interesaba el tema de comunicaciones. Al poco tiempo, también entró Nicolás Baumgarten como becario a la

[11] Novick, F. "Una Red, un día: antes de Internet en Argentina", *Revista de Tecnología e Informática Histórica*, vol. 3, N.º 1, Fundación Museo ICATEC, 2013.

[12] Varsavsky, O. *Hacia una política científica nacional*, Buenos Aires, Ediciones Periferia, 1972.

[13] Una PC con procesador Intel 8086 (NEC APC III) y de un equipamiento de NCR Tower con procesador 68000.

[14] Significa copia de Unix a Unix y es una serie de programas que permiten transferir archivos y ejecutar programas como correo electrónico entre equipos que estén corriendo este sistema operativo (o que soporten este protocolo y programas). La red UUCP es una de las tantas antecesoras que irían a confluir en la gigante Internet. Novick, F. "Un cuartito con vista al mundo", *Radar*, *Página 12*, 18 de mayo de 2014.

> empresa. Este fue el embrión de un grupo que quería hacer investigación en esta área, explorar las capacidades que tenía tanto el X.25 como protocolo, como la herramienta Unix to Unix Copy Protocol (UUCP) como esquema de transferencia de archivos o de información.[15]

Estos espacios fueron los primeros pasos de un equipo que comenzó un largo proceso que sentó las bases para el desarrollo de Internet en Argentina. Con una impronta basada en la autoformación, el ensayo y error, se comenzó a trabajar en el proyecto que devendría en la Red Académica Nacional (RAN), la red de servicio de correo electrónico, sin fines de lucro y de carácter cooperativo entre los centros de investigación científica y tecnológica. La red construyó un sólido grupo de apoyo dentro de la Facultad de Ciencias Exactas y Naturales de la UBA, lo que generó las condiciones propicias para comenzar a desarrollar la tecnología de correo electrónico en el país. La dinámica de colaboración que se gestó en aquel momento entre los diferentes organismos permitió que posteriormente también se incorporara la Cancillería Nacional. Dunayevich afirma:

> En aquel momento, además, conseguimos una cinta magnética de carrete que tenía los códigos fuente de UNIX versión 6. Me interesaba utilizarla para la materia que estaba dando en la facultad. Sin embargo, para poder acceder a la información, tenía que encontrar a alguien que tuviera una unidad lectora de cinta. Así fue que empezó el vínculo con Cancillería.[16]

El proyecto apoyado por el Programa de Naciones Unidas para el Desarrollo (PNUD), que tuvo lugar en la Cancillería durante estos años, buscaba la modernización e informatización del organismo, una iniciativa clave que determinó el interés de quienes lo promovían por trabajar en la incorporación de nuevas tecnologías. En 1986 Alberto Mendelzon, especialista en bases de datos e inteligencia artificial, realizó un viaje al país, y aprovechando el año sabático que le otorgó

[15] Dunayevich, J. y F. Novick. "Orígenes de Internet en Argentina. Un testimonio de Julián Dunayevich", II SHIALC, Medellín, XXXVIII Clei, octubre de 2012.

[16] López, M. P. "Las idas y vueltas de la ciencia. Emigración de científicos y políticas públicas en Argentina", web de la Universidad Nacional del Centro de la Provincia de Buenos Aires [http://bit.ly/2nedM7I].

su lugar de trabajo (la Universidad de Toronto), se sumó al proyecto. Él tuvo la responsabilidad de armar un equipo de trabajo en el que incorporó a Carlos Mendioroz, Jorge Amodio y Mauricio Fernández, y que fue consolidando los lazos entre la Cancillería y la facultad. Mendelzon tenía un especial interés en conectarse con la Universidad de Toronto; logró establecerse la primera comunicación internacional por correo electrónico vía UUCP a comienzos de 1987. Al respecto, Amodio explica:

> El proyecto de Cancillería no tenía que ver con Internet […]. El objetivo principal era modernizar la infraestructura de informática y telecomunicaciones del Ministerio de Relaciones Exteriores y armar una red global con las embajadas y consulados[17].

En el marco de este esquema, se acordó con Sergio Porter, coordinador del PNUD en aquel momento, que la RAN recibiera todos los correos electrónicos del ámbito académico y, por su parte, la Cancillería gestionara aquellos que se enviaban al exterior, debido a que era la única que contaba con un enlace y podía asumir los altos costos que implicaba. Su nodo o punto de interconexión se bautizó Atina. El Departamento de Computación de la FCEyN de la UBA se conectaba a través de otro equipo llamado DCFCEN. En Cancillería Carlos Mendioroz se encargó de gestionar todo lo necesario para que funcionasen en Xenix[18]. Comenzó a realizar llamadas a la Universidad de Toronto y en 1987 generaron la primera conexión periódica de correo electrónico con UUCP. Cancillería recibió el correo para uso interno y DCFCEN comenzó a distribuir el correo a centenas de nodos en el país. Jorge Amodio rememora el momento en que las dos instituciones hicieron contacto:

[17] Op. cit. nota 15.

[18] En 1980, Microsoft introdujo el sistema XENIX, una variante de UNIX, diseñado para ser ejecutado sobre microcomputadoras y computadoras personales, capacidades que sólo estaban disponibles en las grandes computadoras. Almeida Rodríguez. Introducción al Uso del Sistema Operativo Unix: Conceptos Básicos, Tenerife, Universidad de la Laguna.

> Contando con Atina lista para prestar servicio, informalmente le solicitamos permiso a la coordinación del proyecto de informática de Cancillería para crear una cuenta en Atina con el objeto de establecer una conexión con el Departamento de Computación de Exactas[19].

4. El avance de las conexiones por correo electrónico antes de Internet

Desde el año 1987, cuando se envió la primera comunicación internacional por correo electrónico vía el protocolo UUCP, nuestro país fue centro de disputa, ya desde sus orígenes, de dos modelos de trabajo que tenían en su esencia visiones e intereses contrapuestos. Por un lado, la red BITNET,[20] que contaba con conexiones en la Universidad de La Plata y en la CNEA (Comisión Nacional de Energía Atómica), y por otro lado, el despliegue de la red UUCP, impulsado principalmente por algunos actores de la academia y por sectores que formaban parte de los proyectos de tecnología fomentados por Cancillería. Estos modelos en pugna también se diferenciaron en los caminos que recorrieron a lo largo de su desarrollo a escala nacional y regional. Mientras que la red BITNET requería accesos en línea y equipos grandes y potentes para el procesamiento de datos, la red UUCP contaba con equipamiento más pequeño, con mayor capacidad de capilaridad, y distribuido por distintos puntos de la región, lo que reafirmó un modelo de trabajo que consistía en fortalecer la dinámica de inclusión a escala país.[21] Julián Dunayevich lo cuenta de la siguiente manera:

> Íbamos armando los nodos UUCP conectados a nuestro nodo [DCFCEN] y nos encargábamos de registrarlos uniendo lentamente diferentes centros de investigación y universidades. Dentro de la Universidad de Buenos Aires conectamos primero toda la Facultad de Ciencias

[19] Op. cit. nota 17.
[20] BITNET nació en 1981 dentro del ámbito académico estadounidense. Utilizó el protocolo de IBM llamado RSCS. Su objetivo era la comunicación entre el campo académico mediante el uso de una la línea telefónica. Amodio, J. "Internet vs. Bitnet", Internet Argentina, Historia y evolución (blog), 2010 [http://bit.ly/2naQuzL].
[21] Op. cit. nota 16.

> Exactas y Naturales, luego la de Ingeniería, y el resto de las facultades para que tuvieran correo electrónico. Le dimos conexión a la Escuela Superior Latinoamericana de Informática (ESLAI), conectamos a La Plata… Argentina llegó a contar con más de ochocientas instituciones conectadas vía UUCP[22].

En un primer momento los países que estaban conectados con la red UUCP construyeron mapas donde podían observarse las diferentes computadoras que se encontraban conectadas en el ámbito mundial[23]. UUNET reunía los mapas y a su vez los distribuía. En el marco de este esquema, fueron creados los "pseudo-dominios" .BITNET, .CSNET y .UUCP, entre otros. Según dichos de Amodio:

> Alberto sugiere que como diminutivo de Argentina podíamos utilizar "atina!", exactamente seis caracteres, representaba su ubicación y sonaba bien. Configuramos la máquina con este nombre y comenzamos a llamar con UUCP a "utai", que representaba al Departamento de Inteligencia Artificial de la Universidad de Toronto, con el que Alberto estaba asociado. Alberto recibe los primeros mensajes de correo electrónico a su dirección ahora en Argentina, utai!atina!mendel. Era práctica común que, para crear los nombres de usuarios, algunos utilizaran las iniciales que representaban su nombre, otros su nombre de pila o algo que fuera combinación del nombre de pila y apellido, pero lo más tradicional era inventarse un *nickname* o alias.[24]

De este modo, se definieron en cada red algunos nodos en particular que actuarían como puentes para el intercambio de mensajes entre distintas redes. UUNET se convirtió en la puerta de enlace principal para UUCP. Utilizando este sistema fue posible sustituir el esquema de direcciones de correo electrónico de, por ejemplo,"utai!atina!dcfcen!maria" a maria@dcfcen.uucp. Carlos Mendioroz era el responsable de administrar los mapas de UUCP

[22] Op. cit. nota 15.
[23] Amodio, J. "Nace Atina", Internet Argentina, Historia y evolución (blog), 2010 [http://bit.ly/2oDM8Br].
[24] Op. cit. nota 21.

en Argentina. Esta red, también conocida como USENET,[25] tuvo un crecimiento exponencial, tal como afirma Jorge Amodio, "llegando a mediados de los años ochenta a contar con varias miles de máquinas interconectadas utilizando UUCP"[26]. Junto con la instalación de la Microvax se conectaron varias líneas telefónicas adicionales. Ese proceso llevó a que Carlos Mendioroz asumiera el rol de "postmaster" de Atina y que se pusiera en contacto con Rick Adams, que era el administrador de "seísmo",[27] uno de los nodos que se ubicaban en el Estado de Virginia. Y como resultado de esta relación que se constituyó, Argentina pudo acceder a una conexión desde Atina a seísmo. Jorge Amodio recuerda ese momento de la siguiente manera: "Ahora nuestras direcciones de correo incluían nuestra ruta alternativa como: {seismo|utai}!atina!usuario"[28]. Esta situación derivó en un crecimiento exponencial de USENET, dejando en evidencia la necesidad de que algún otro mecanismo pudiera ordenar la ruta que iban a seguir los mensajes de origen a destino. Jorge Amodio afirma con estas palabras esa situación:

> A mediados de los años ochenta se inició el proyecto UUCPMAP, que simplemente establece un formato estándar para representar a cada nodo y distribuir esta información al resto de la comunidad que formaba parte de USENET. De esta forma era posible construir un mapa lógico de la red y por medio del programa utilitario llamado "pathalias" generar una lista de rutas a seguir para cada destino.[29]

Es así como Atina se convierte en el primer nodo concentrador de USENET en Argentina. El resto de los nodos incorporaban sus mapas para también usar el mismo esquema de direcciones.

Aquellos países que usaban el protocolo TCP/IP utilizaban el archivo conocido como HOST.TXT,[30] que consistía en armar un listado don-

---

[25] Kirch, O. y T. Dawson. *Guía de Administración de Redes con Linux*, Sebastopol, California, O'Reilly & Associates, 2000 [http://bit.ly/2naThZJ].
[26] Op. cit. nota 26.
[27] Burgess, J., M. Jahr, J. Keljo, J. Schroeder & W. Sweitzer. "The Great Renaming" [https://stanford.io/2mm8Z3K].
[28] Op. cit. nota 26.
[29] Op. cit. nota 26.
[30] Mockapetris, P. "Nombres de dominio. Conceptos e instalación", Request for Comments:

de a un *host* se lo asociaba con una dirección IP. Este formato permitía administrar de manera manual los nombres mapeados a números. En 1984 ya se había propuesto la implementación del Sistema de Nombres de Dominio (DNS) para organizar los nombres de los *host*, en una forma jerárquica y con un mecanismo de resolución distribuido. Comienza entonces la transición del viejo archivo HOSTS.TXT al nuevo sistema. Dos años más tarde se organizó una reunión de coordinación entre las distintas redes académicas que representaron a la comunidad de los usuarios de la red UUCP. Es en el marco de ese encuentro Mark Horton sugirió la creación de un "pseudo-dominio" para distinguir en forma transitoria a los nodos que formaban parte de la red USENET. Fue el 29 de julio de 1987 que Carlos Mendioroz envió el registro para incorporar a Atina en los mapas de la red UUCP.

Con el transcurso del tiempo, comenzó a utilizarse el Sistema de Nombres de Dominio (DNS), que permitió elaborar un diagrama de distribución donde, por un lado, existieran dominios genéricos de primer nivel o Top Level Domain (gTLDs), tales como ".com", ".net" y ".org", y los llamados Country Code Top Level Domain (ccTLDs), es decir, los dominios de primer nivel de código de cada país tales como ".ar", ".br" y ".cl". Oscar Sznajder afirma en su testimonio:

Poco después de comenzar con esa distribución de los archivos por UUCP viene el momento de la creación del dominio. La creación del dominio argentino es el primero de Latinoamérica.[31]

El 23 de septiembre[32] [33] de 1987 fue un hito para la historia de las redes en Argentina, ya que Carlos Mendioroz registró el Top Level Domain, el dominio de más alto nivel, utilizando el código de dos letras predefinido para el país en el estándar ISO-3166-1 (.AR), y quedó establecido de allí en más. El objetivo principal era poder mantener la comunicación con el exterior a través del correo electrónico y que, a su vez, se mantuvieran ordenados y organizados los mapas de la red UUCP para Argentina para saber qué destinos se encontraban disponibles en el país.

1034 [http://bit.ly/2oKgCSF].

[31] Sznajder, Oscar, 2017. Ver anexo.

[32] Ver: https://www.iana.org/domains/root/db/ar.html.

[33] Jorge Amodio recuperó el mail original de registro de dominio en: http://bit.ly/2o0yjgo.

> El primer dominio que creamos bajo .AR fue "MREC.AR", justamente para el Ministerio de Relaciones Exteriores y Culto. Poco tiempo después, una vez que con Julián Dunayevich y Nicolás Baumgarten en el Departamento de Computación de la Facultad de Ciencias Exactas y Naturales le damos vida a nuestro primer nodo UUCP en el sector académico, el 13 de noviembre de 1987 le envié a Carlos Mendirioz el registro de DCFCEN para ser incorporado en los mapas UUCP y convertirse en el primer nodo bajo el subdominio ".EDU.AR".[34]

Esto posibilitó que las direcciones de correo electrónico fuesen más estables al quedar la conexión de UUNET con Atina como puerta de enlace principal para los mensajes que tuvieran como destino cualquier nodo que terminara con ".ar". Seguíamos conectados vía UUCP pero seísmo funcionaba como *gateway* a Internet.

Si bien la creación del ".ar" y del DNS podría parecer anecdótica, estos hechos históricos pueden demostrar los resultados de un trabajo colectivo y colaborativo entre diferentes actores. Si bien aún no existía formalmente NIC Argentina como institución, estos acontecimientos permitieron, por un lado, dar al registro de los primeros nombres de dominio con impronta nacional, sentando las bases de lo que sería su posterior desarrollo, y por otro, dar origen a la administración de una infraestructura crítica.

5. Los noventa marcan el auge del correo electrónico y el camino a Internet

La década de 1990 dio inicio a una nueva etapa en la política argentina, con transformaciones que modificaron al país económica y políticamente. En el año 1990 comenzó el proceso de privatización de ENTel, la empresa pública de telefonía, hecho que marcó el inicio de una contienda más grande: definir quién se quedaba con la administración de las redes y quién iba a controlarlas. El mapa ya era más extenso y había muchos más intereses en juego que en los primeros días.

[34] Amodio, J. "GOV.AR o GOB.AR, Mea Culpa", Internet Argentina, Historia y evolución (blog), 2010 [http://bit.ly/2naOesh].

A medida que se fueron incorporando actores que no pertenecían sólo al ámbito académico, empezaron ciertos debates sobre cómo debía establecerse lo que hoy conocemos como Internet en el país. El 17 de mayo de 1990 Carlos Mendioroz y Jorge Amodio lograron establecer el primer enlace analógico, habilitando el intercambio de mensajes a través de UUCP y dando los primeros pasos para lograr una conexión a Internet en Argentina.

Se estaba haciendo evidente lo importante y necesario que era encuadrar las diversas iniciativas dentro de un marco institucional. Julián Dunayevich rememora:

Había que bajar el nivel de voluntarismo y empezar con una estructura real, que era la única forma de continuar el proyecto. Estábamos todos contentos, recibíamos centenares de cartas apoyándonos, pero no servía en términos institucionales, no podíamos asentar todo lo conseguido y de alguna forma nos sentíamos estancados[35].

En septiembre de 1992 el Consejo Superior de la UBA creó la Red de la Universidad (RedUBA) y el Centro de Comunicación Científica (CCC)[36] para administrarla. Dunayevich recuerda:

> Fue un hito importantísimo porque fue la primera institucionalización de todo lo que estábamos haciendo: pensar en una red metropolitana para toda la universidad con personal estable, con un espacio y presupuesto[37].

El 8 de abril de 1994 la Universidad de Buenos Aires pudo obtener el primer enlace digital de Internet en nuestro país a través de Telintar, que era el brazo internacional de Telecom y Telefónica. Así, la universidad pudo ingresar a la red marcando un momento trascendental para la historia de Internet en Argentina y un hito para la historia de NIC.ar, ya que se logró conectar a todo el sector académico a Internet, quedando la administración del dominio '.edu.ar' en manos, primero, de la Universi-

[35] Dunayevich, J. y F. Novick. "Orígenes de Internet en Argentina: segunda parte. Un testimonio de Julián Dunayevich, Nicolás Baumgarten y Mauricio Fernández", Memorias del III Simposio de Historia de la Informática de América Latina y el Caribe (SHIALC 2014), Uruguay, 2014.
[36] La resolución de su creación puede ser relevada en: http://bit.ly/2n1LMV7.
[37] Op. cit. nota 32.

dad de Buenos Aires, y luego, de la Red de Interconexión Universitaria (RIU). La institucionalización de este proceso permitió que se pudieran profundizar los vínculos y formar sólidos equipos de trabajo: el impulso que brindaron los sectores académicos para el desarrollo de Internet atravesó los límites de la Ciudad de Buenos Aires, ya que jóvenes de otros puntos del país lograron obtener enlaces propios para la Universidad Nacional de La Plata y la Universidad Nacional de Córdoba. También la propia Cancillería.

En aquellos primeros tiempos, ya era grande la demanda que se presentaba de los ".com.ar", y como aún no existía formalmente NIC Argentina, el registro de dominios se realizaba de manera sencilla en una planilla de Excel en el espacio de la Cancillería. No obstante, esta acción era llevada meticulosamente por parte del equipo que trabajaba en el área de desarrollo, no sólo para poder seguir un orden sino también para evitar cualquier inconveniente de índole legal[38]. Finalmente, en los primeros meses de 1994 se formalizó la fundación de NIC Argentina como organismo reglamentado y con facultades para el registro de los dominios ".ar".

En la Argentina se daban distintas corrientes de pensamiento: algunos pensaban que era importante que el Estado, a través del brazo de la Cancillería, se hiciera cargo de la administración del registro de dominio, mientras que otras voces proponían que fuera el sector académico el que asumiera dicha función. Aquellos que pensaban que era la Cancillería la que debía hacerse responsable, sostenían su argumento a partir de la idea de que era importante contar con representantes que tuvieran autoridad, conocimiento del tema y capacidad política de intervención. Se asumió que era importante que el ".ar" como parte de la identidad nacional quedara en manos del Gobierno argentino, sentando un antecedente en el continente latinoamericano y diferenciándose de otros modelos de gestión regionales donde prevalecían la gestión privada y la tercerización.

Paralelamente al crecimiento sostenido del registro de dominios que atravesaba Argentina, sucedió otro acontecimiento crucial: Internet logró

[38] Jorge Amodio recuperó los primeros formularios de registro de dominio en http://www.amodio.biz/jorge/inetar/docs/dom002-1991-sp.pdf.

traspasar las fronteras académicas para ingresar en el mundo comercial. Fue en 1995, más precisamente en el mes de abril, cuando se vendieron las primeras conexiones comerciales a Internet. A partir de ese momento Internet comenzó un largo proceso de transformación donde el mayor impulso fue dado por las empresas, que tenían un interés comercial.[39]

6. La consolidación de un modelo de trabajo

Poco a poco, el alcance de la red se expandió y generó la necesidad de comenzar a trabajar con diversos países de la región, compartiendo experiencias y conocimientos entre sí y superando barreras geográficas. En este marco, en marzo de 1991 se llevó a cabo en Chile la reunión de SIRIAC, el Sistema Interconectado de Recursos Informativos Académicos y Científicos, en el que participaron distintos países latinoamericanos con el objetivo de crear una red regional, pensada en aquel entonces para el ámbito académico. Gracias a este impulso, en octubre de ese mismo año se realizó el primer Foro de Redes de América Latina y el Caribe en Río de Janeiro, Brasil, en el Instituto de Matemática Pura y Aplicada (IMPA), que contó con la participación de la mayoría de los países de la región y de una gran cantidad de organismos internacionales. En este contexto también se dio origen a EnRED, la entidad que nucleó a las diferentes universidades y centros de investigación de la región para promover una mayor conectividad en los países y generar espacios de capacitación.

Las experiencias demostraban que se debía generar una comunidad más amplia en la que participaran nuevos actores. En el contexto internacional, esto generó las condiciones propicias para la formación de la organización Internet Society en 1992, en Copenhague, Dinamarca. En América Latina se vivía el mismo espíritu. En octubre de 1997, en el Foro de Redes de América Latina y el Caribe realizado en La Habana, Cuba, un grupo de académicos vislumbró que para poder darles una estructura más formal a los diferentes desafíos y problemáticas que Internet esbozaba, era necesario realizar trabajar con otros actores, principalmente con las nacientes empresas.

[39] Soriano, J. "Historia de Internet en Argentina: 1995", Historia de Internet en América y el Caribe [http://bit.ly/2nVz0HC].

> Si bien la mayoría de los pioneros, por llamarlos de alguna manera, en esta discusión seguimos estando involucrados en este proceso, creo que fue muy importante el carisma aglutinador de ese pequeño grupo que entendió que no había otra alternativa que abrir y juntar gente. Lo digo porque en algún momento nosotros no teníamos esa visión y nos dimos cuenta de que teníamos que cambiar.[40]

Años más tarde, en 1998, se creó Latin American and Caribbean ccTLDS Organization (LACTLD), que comenzó a agrupar a las diferentes instituciones que administraban dominios de primer nivel dentro de los países de la región. Un año después, en agosto de 1999, nació LACNIC, el Registro Regional de Internet para América Latina y el Caribe, una institución que tenía como objetivo empezar a distribuir dichas direcciones IP en la región, sin tener que depender de ARIN (Registro Americano de Números de Internet). Pero más allá de dicha función práctica, ya desde aquel momento se proponía ser un organismo global que fuera un catalizador para el desarrollo de Internet en la región y que generara capacidades al interior de la comunidad.

De esta manera, se hace visible cómo durante los últimos años de la década de 1990 se fue consolidando un modelo de trabajo basado en la colaboración de una diversidad de actores y en la consolidación de instituciones formales, generando las condiciones propicias para el desarrollo de nuevo concepto que comenzó a utilizarse para hacer referencia a estos temas de discusión, el de Gobernanza de Internet.

7. La evolución de NIC Argentina

El auge constante del crecimiento de Internet que estaba dándose en el país puede verse en el incremento que se dio en el número de registros de dominios en NIC Argentina entre los años 1996 y 1997, ya que se produjo un

[40] Graizer, Ariel, 2017.

aumento del 974%[41]. El trámite de registro[42] era gratuito, lo que favoreció el crecimiento de dominios pero, por otro lado, también se abrió una puerta para la especulación de registradores que buscaban obtener un beneficio económico por la reventa de nombres de dominios considerados interesantes.

El 8 de agosto de 2000, con el objetivo de robustecer el marco legal y actualizarlo a los parámetros internacionales, se firmó la Resolución 2226/2000,[43] que aprobó e hizo públicas las reglas para el registro de nombres de dominio en Argentina. A partir de este momento histórico la reconstrucción de la evolución de NIC Argentina se dificulta debido a la falta de fuentes fidedignas. Recién se vuelve a contar con información certera sobre la institución a partir de 2011, año en el que comenzó una nueva etapa para la organización, ya que por el Decreto Presidencial 2085/2011[44] se creó la Dirección Nacional del Registro de Dominios de Internet, dentro del ámbito de la Secretaría Legal y Técnica de la Presidencia de la Nación, la cual tendría como función administrar este recurso de Internet.

A partir de ese momento, se dotó al organismo de una estructura organizativa que permitiera abordar adecuadamente sus necesidades técnicas y operativas, y durante los años siguientes se tomaron diversas medidas para optimizar la información del registro y la administración del .ar. Puntualmente, el 20 de agosto de 2013, con el objetivo de desalentar la inscripción de dominios con fines especulativos, se implementó el arancelamiento del servicio, sumándose así a las diversas recomendaciones internacionales que se hacían en relación a la materia. Para ese entonces, Argentina era uno de los pocos países que aún no cobraban por el servicio; una vez aplicado el plan, la cantidad de registros bajó, pasando de tener 2.500.500 a 500.000 dominios[45]. De este modo pudo lograrse con éxito el objetivo de tener disponibles para la comunidad dominios que habían sido reservados por personas que especularon a través de la reventa, dado el particular interés que generaban algunos nombres.

---

[41] Dandan, A. "Traficantes de nombres", *Radar*, *Página 12*, 2 de septiembre de 2001 [http://bit.ly/2n2fF7I].

[42] El reglamento vigente de NIC Argentina para dicho momento se puede relevar de: http://bit.ly/2oEcyTG.

[43] Puede relevarse en: http://bit.ly/2n1O46F.

[44] Puede relevarse en: http://bit.ly/2mnyFwV.

[45] NIC Argentina. "30 años de NIC Argentina", 2017 [http://bit.ly/2o0C6KE].

En los últimos tiempos, principalmente desde 2016 y hasta la actualidad, se propuso construir un nuevo paradigma de trabajo y nuevas metas para NIC Argentina que, bajo dos grandes lineamientos, permitiera impulsar de manera constante el crecimiento de Internet en Argentina y aumentar la confianza de la sociedad en la red. Bajo este paradigma lleva adelante proyectos de innovación tecnológica para administrar de manera eficiente el registro de nombres de dominio, asegurar el funcionamiento del DNS (Sistema de Nombres de Dominio) para el Dominio de Nivel Superior Geográfico ".ar" y promover el crecimiento de Internet. Algunos de los proyectos destacados son la Red Anycast, que busca robustecer la infraestructura crítica, el DNS, y la Coalición IPv6, de la que forma parte y que pretende promover el despliegue de la nueva versión del protocolo de Internet, en pos de favorecer la conectividad de un número cada vez mayor de dispositivos. Además, siguiendo la línea de trabajo, participa activamente en los debates sobre Gobernanza de Internet y genera espacios que propicien la difusión y puesta en práctica de estas discusiones, lo que habilita, a su vez, a consolidar los vínculos existentes y generar nuevos dentro de la comunidad de Internet. Entre ellos se destaca que desde 2017 realiza el ciclo de Charlas Debate sobre Gobernanza de Internet, un evento que busca generar el debate de temas vinculados a Internet de impacto en nuestro país y para el cual generó ya cuatro ediciones. También es de destacar la iniciativa Blockchain Federal Argentina (BFA), de la que es parte, que desde sus cimientos se forjó bajo una lógica de trabajo colaborativo entre las múltiples partes interesadas. Con su premisa de la continuidad, la BFA trabaja en un modelo que permite que la plataforma habilitada por la tecnología perdure más allá de las personas e instituciones que la gestaron. Si bien es pronto para establecer conclusiones, promete optimizar diferentes tipos de procesos, servicios y aplicaciones de los sectores más diversos.

8. Conclusiones

Si bien esta investigación realizó un recorrido histórico del surgimiento de Internet en nuestro país y del nacimiento de NIC Argentina, el anhelo con este trabajo no es darle un cierre a la historia, sino aprender del

pasado para trabajar en el presente y pensar en el futuro, pero no sólo de NIC Argentina sino de Internet.

Hemos visto que a través de los años un modelo de gestión de recursos se fue formalizando, no solamente en NIC Argentina sino a lo largo de toda la comunidad de Internet, y es el modelo que justamente la concibe como ecosistema, como un conjunto de partes con recursos, miradas o experiencias diferentes, pero todas esenciales, todas reconociéndose recíprocamente como interesadas en el futuro de la red. Esta formalización puede haberse consolidado definitivamente con el nacimiento de aquellos espacios internacionales que ya se han analizado, pero el rumbo ya estaba marcado desde un principio. Porque el avance de Internet, por más que haya parecido dominio de uno u otro sector en determinado momento, siempre estuvo alimentado por la discusión, por la cooperación e incluso por la competencia entre esas partes. Por eso es esencial entender que el camino que llevó a la gestión de los dominios y la aparición de NIC Argentina como actor fundamental en esta comunidad, es el camino del intercambio entre las partes de esta comunidad. Y no ha dejado de serlo.

Es en este contexto donde la expresa intención de participar y aportar en las discusiones de los diversos temas que forman parte de la cultura de Internet, de incentivar y fortalecer la comunidad, debe ser entendida. Al reconocerse no sólo como parte de una infraestructura crítica sino como actor de ese ecosistema de Internet, NIC Argentina no sólo refuerza este paradigma sino que encara las responsabilidades que esto implica.

Por ello, el compromiso por abrir espacios de discusión o generar iniciativas tecnológicas que trasciendan la gestión del DNS debe leerse en esta clave histórica. La gesta de la computación científica en nuestro país, la evolución de las redes, los proyectos colaborativos entre Estado y Academia, los debates para consolidar un modelo de red de redes, toda la historia de Internet ha moldeado este modelo de colaboración entre partes interesadas, y es imprescindible volver a analizarla en este código para reafirmar este camino de una institución que, como muchas otras, se reconoce parte de una comunidad y trabaja día a día para consolidarla.

Referencias

Aguirre, J. "Panorama de la historia de la Computación Académica en la Argentina", *Historia de la Informática en Latinoamérica y el Caribe: Investigaciones y Testimonios*, Río Cuarto, Universidad Nacional de Río Cuarto, 2009.

Almeida Rodríguez. *Introducción al Uso del Sistema Operativo Unix: Conceptos Básicos*, Tenerife, Universidad de la Laguna,

Amodio, J "GOV.AR o GOB.AR, Mea Culpa", Internet Argentina, Historia y evolución (blog), 2010 [http://bit.ly/2naOesh].

—"Internet vs. Bitnet", Internet Argentina, Historia y evolución (blog), 2010 [http://bit.ly/2naQuzL].

—"Los primeros pasos", Internet Argentina, Historia y evolución (blog), 2010 [http://bit.ly/2oDM8Br].

—"Nace Atina", Internet Argentina, Historia y evolución (blog), 2010 [http://bit.ly/2oDM8Br].

Blanco, E. "50 años de la carrera de computador científico, en la UBA", Blog Portinos, 2013 [http://bit.ly/2naStEc].

Burgess, J., M. Jahr, J. Keljo, J. Schroeder & W. Sweitzer. "The Great Renaming" [https://stanford.io/2mm8Z3K].

Czemerinski H. & P. M. Jacovkis. "La llegada de la computación a la Universidad de Buenos Aires", *Revista Iberoamericana de Ciencia Tecnología y Sociedad*, vol. 6., N.º 18, Ciudad Autónoma de Buenos Aires, agosto de 2011

Dadan, A. "Traficantes de nombres", *Radar*, *Página 12*, 2 de septiembre de 2001 [http://bit.ly/2n2fF7I].

Dunayevich, J. y F. Novick. "Orígenes de Internet en Argentina. Un testimonio de Julián Dunayevich", II SHIALC, Medellín, XXXVIII Clei, octubre de 2012.

—"Orígenes de Internet en Argentina: segunda parte. Un testimonio de Julián Dunayevich, Nicolás Baumgarten y Mauricio Fernández", Memorias del III Simposio de Historia de la Informática de América Latina y el Caribe (SHIALC 2014), Uruguay, 2014.

Ferreyra, G. *Internet paso a paso: hacia la autopista de la información*, México, Alfa Omega, 1996.

Kirch, O. y T. Dawson. *Guía de Administración de Redes con Linux*, Sebastopol, California, O'Reilly & Associates, 2000 [http://bit.ly/2naThZJ].

López, M. P. "Las idas y vueltas de la ciencia. Emigración de científicos y políticas públicas en Argentina", web de la Universidad Nacional del Centro de la Provincia de Buenos Aires [http://bit.ly/2nedM7I].

Mockapetris, P. "Nombres de dominio. Conceptos e instalación", Request for Comments: 1034 [http://bit.ly/2oKgCSF].

Novick, F. "Un cuartito con vista al mundo", *Radar*, *Página 12*, 18 de mayo de 2014.

—"Una Red, un día: antes de Internet en Argentina", *Revista de Tecnología e Informática Histórica*, vol. 3, N.º 1, Fundación Museo ICATEC, 2013.

Soriano, J. "Historia de Internet en Argentina: 1995", *Historia de Internet en América y el Caribe* [http://bit.ly/2nVz0HC].

Swann, B. "The Ferranti Computer Department", unpublished notes, 1975.

Varsavsky, O. *Hacia una política científica nacional*, Buenos Aires, Ediciones Periferia, 1972.

Buscadores de Internet, palabras clave y uso de marca ajena

por Javier Alejandro Papaño

1. Breve noción de los hechos y del caso

La sentencia de la Sala III de la Cámara Nacional de Apelaciones en lo Civil y Comercial Federal en el caso "Organización Veraz v. Open Discovery"[1] hace un relevamiento muy bien detallado y circunstanciado de los antecedentes de la causa y de los hechos sometidos a juzgamiento. Por tal motivo, vamos a limitar al mínimo posible las referencias a los antecedentes y hechos, remitiendo al lector a la fuente directa, el fallo.

Sí aclaramos que lo que se debatió en la causa es si el uso de la marca de un competidor como palabra clave (*keyword*) en los buscadores de Internet, con la finalidad de atraer clientela, constituye una infracción marcaria en los términos de la Ley N.º 22.362, y un acto de competencia desleal; y si dicho ilícito puede generar consecuencias dañosas susceptibles de ser reparadas.

Eso es lo que hizo la demandada. Utilizó como palabras clave en los motores de buscadores de Internet las marcas VERAZ y ORGANIZACIÓN VERAZ de la actora, además de otras denominaciones similares como VERAS, BERAZ y BERAS. Como consecuencia de ese uso, ante el ingreso en los cuadros de búsqueda de tales términos por los usuarios de Internet, logró aparecer en los resultados con enlaces patrocinados, con preferencia respecto de los resultados naturales que conducían al sitio y servicios de la actora.

Desde el punto de vista tecnológico, probablemente el fallo bajo análisis no se refiera a hechos novedosos. Pero desde la óptica del Derecho es de gran trascendencia, ya que es el primero en resolver sobre esta cuestión, lo cual no es un tema menor, toda vez que el Derecho suele correr en desventaja respecto de los hechos, pues estos últimos acontecen primero, sobre todo en cuestiones en las que el vertiginoso avance de la

[1] CNFed. CC, Sala III, causa 1789/09, 4/5/18, "Organización Veraz SA c/ Open Discovery SA s/ cese de uso de marca". Ver texto de la decisión publicado en la sección "Jurisprudencia" de este número de la revista, p. 344.

tecnología y las ciencias desafían la inteligencia de las categorías jurídicas tradicionales.

2. Los fundamentos del fallo

El principal acierto del fallo, en nuestra opinión, es considerar que el uso de la marca ajena como palabra clave (*keyword*) por un competidor constituye una infracción. Para llegar a esa conclusión, la doctora Medina —vocal preopinante— recurre, en una primera aproximación al tema, al Derecho comparado mediante el análisis de algunos casos fallados por cortes de Estados Unidos de América y por el Tribunal de Justicia de la Unión Europea. Si bien la incidencia de las conclusiones de fallos foráneos es relativa, pues se nutren de principios y normas que muchas veces no son coincidentes con las locales, en casos novedosos permiten analizar y ponderar los argumentos fácticos y jurídicos que sustentan una y otra posición para confrontarlas con nuestro Derecho interno.

Las distintas hipótesis del uso de una marca por quien no es su titular han dado lugar a una distinción o categorización. Así, se distingue entre el uso de una marca ajena como propia y el uso de una marca ajena como ajena[2]. No hay lugar a dudas de que la conducta de quien utiliza la marca de un tercero como propia, es decir, para identificar los productos que fabrica y vende o los servicios que presta, constituye infracción, y está alcanzada por el artículo 31, inciso *a* de la Ley de Marcas. Este uso afecta la principal función de la marca, la distintiva, aunque también una de las secundarias, la de indicación de origen o procedencia. La duda se genera en los otros supuestos, es decir, aquellos en los que el tercero que usa la marca lo hace bajo el reconocimiento de que se trata de una marca ajena, o bien la utiliza como un factor de atracción para potenciar el uso de sus marcas propias.

Dentro del segundo supuesto también es posible advertir diferentes escenarios. No todo uso de una marca ajena es ilícito, lo que equivale a decir que existen usos lícitos de la marca ajena. Entre estos últimos podemos citar el uso por revendedores o distribuidores, el uso para indicar

[2] También suele hablarse de uso marcario y no marcario, y algunos autores se refieren a los usos típicos y atípicos (ver Bertone, Luis E. y Guillermo Cabanellas de las Cuevas, *Derecho de Marcas*, Buenos Aires, Heliasta, 2003,. T. 2, p. 244 y ss.).

compatibilidad con repuestos o accesorios, y el uso relacionado a servicios técnicos o de reparación. Si estos usos no sugieren la existencia de un vínculo o asociación entre el tercero y el titular de la marca, no aprovechan indebidamente el prestigio o el poder de atracción de la marca ajena, y no dañan o denigrar su reputación o distintividad, no se produce interferencia con el ámbito de protección que confiere la marca.

En síntesis, a la marca se le reconocen como funciones la distintiva, la de indicación de origen, la publicitaria o poder de atracción, y la de garantía, y es en virtud de dichas funciones que debe ser tutelada. Por lo tanto, cualquiera de los usos que hemos mencionado, en la medida en que afecte una o varias de las funciones de la marca, podrá ser considerado contrario a Derecho, cuestiones que no profundizamos aquí, pues excederían largamente el propósito de este comentario.

En el fallo ha quedado bien claro —y esto también lo consideramos un acierto— que la demandada es competidora directa de la actora, y que el uso marcario cuestionado fue con relación a los servicios que prestan ambas partes.

Por ello, también es adecuada la referencia a la competencia desleal, aun cuando las normas que la regulan en nuestro país se caractericen por su escasez y dispersión. En distintos pasajes de la sentencia se deja sentado que la demandada, que ingresó en el negocio de los informes comerciales con bastante posterioridad a la actora, utilizó como palabras clave las marcas de esta última, con el fin de aprovecharse de su prestigio y renombre, garantizándose el acceso a una cartera de clientes con un mínimo costo de inversión y esfuerzo comercial.

La pregunta que cabe hacerse es: ¿cómo habría sido el desempeño comercial y económico de la demandada si hubiera utilizado sus marcas o denominaciones genéricas —como informe comercial o crediticio—? Y tal vez sea posible encontrar la respuesta en la propia conducta de la demandada, que por algo prefirió valerse de las marcas de la actora.

Estas reflexiones, que brindan un gran sustento a la decisión final, permiten conjugar el ilícito marcario con la competencia desleal, en particular con el indebido aprovechamiento del prestigio y del esfuerzo ajeno, aun cuando sean cuestiones que no siempre vayan de la mano. En efecto, toda infracción marcaria dolosa encierra un acto de competencia

desleal, pues la conducta no es más que el aprovechamiento del esfuerzo y prestigio ajeno a través del uso de la marca ajena. Pero los actos de competencia desleal exceden en número y tipo a los ilícitos marcarios,[1] por lo que la ecuación no funciona a la inversa.

Veraz, como marca, como nombre de empresa, como indicación de origen, es una denominación notoria, y por tal motivo es merecedora de una protección especial, acentuada. Esta circunstancia ha sido debidamente reconocida en el fallo, en desmedro de la posición de la demandada, que intentó asimilar los signos distintivos de la actora con signos genéricos carentes de tutela marcaria.

Por último, una reflexión respecto de la cuestión pecuniaria. En materia de infracciones a la propiedad intelectual (la cuestión no sólo se limita a las marcas), tanto la doctrina como la jurisprudencia han puesto de manifiesto las dificultades que encierra la acreditación del daño y del nexo causal, así como la cuantía de aquel. Esas dificultades muchas veces sirvieron de excusa para negar la procedencia de los reclamos resarcitorios. Otras tantas, para reconocerlos en una medida poco significativa, que constituían más un premio al infractor que una reparación al titular de los derechos afectados.

En los últimos tiempos el camino empieza a ser otro, con la vista puesta no sólo en el titular de los derechos, sino también en el infractor y en los beneficios ilícitos obtenidos a partir de la infracción. Este fallo se inscribe en esa tendencia, que es más realista, y que sirve sin lugar a dudas como un llamado de atención, en el sentido de que infringir los derechos ajenos tendrá consecuencias económicas.

3. Conclusiones

Internet, en muchos casos de aquellos que importan al Derecho, es simplemente un escenario, una plataforma digital donde se llevan a cabo las mismas conductas que en el mundo real (los fallos de otros países y las discusiones en el nuestro se nutren de analogías y ejemplos del mundo

[1] Ver Otamendi, Jorge, "La competencia desleal", *Revista Jurídica de la Universidad de Palermo*, Buenos Aires 1998, vol. 3.

real que ayudan a comprender e interpretar las conductas que se llevan a cabo en el mundo virtual). Es cierto que las facilidades de acceso son ilimitadas, y es por ello que es una fuente inagotable de conflictos. Pero también lo es que si las conductas en muchos casos son semejantes, también deben serlo las normas aplicables, y por ende las consecuencias, aun cuando requieran de un esfuerzo interpretativo inédito.

La adopción de una marca ajena como palabra clave no constituye de por sí un acto ilícito. La vida negocial está repleta de ejemplos en los cuales el uso de la marca de otro no es ilícito. Esos mismos ejemplos se replican en el mundo virtual.

La adopción de una marca ajena como palabra clave por parte de un competidor constituye un ilícito marcario, y como tal, un acto de competencia desleal, susceptible de generar el deber de reparar los perjuicios causados.

Por todo lo expuesto en estas breves líneas, saludamos con beneplácito los criterios y fundamentos que informan este fallo que, entendemos, se dirigen en el camino correcto.

Nuevas formas de identificación y autenticación en la nueva economía creada por Internet

por Leonor Guini

Abstract: el presente trabajo tiene por objeto analizar la identificación y la autenticación de las personas en entornos electrónicos, temática esencial para el desarrollo del comercio electrónico y el gobierno digital. Se analizará la validez legal de estas tecnologías reconocidas por el Derecho a la luz de las nuevas necesidades de negocios planteadas por una economía que gira alrededor de Internet.

Veremos el gran desarrollo que la firma digital tiene dentro del sector público nacional y analizaremos las políticas de Estado tendientes a acercar esta tecnología a todos los ciudadanos. Asimismo notaremos, en contraposición, cómo se desarrolló el mercado de firma electrónica en el sector privado y cómo el Estado se fue adaptando a estos nuevos modelos de negocios.

Voces: autenticación, identificación, autenticación biométrica, firma digital, firma electrónica, firma digital remota, identificación digital única, plataforma de firma digital remota, infraestructura de firma digital de la República Argentina, certificados de atributos, política de certificación de la Autoridad Certificante de Modernización que usa Plataforma de Firma Digital Remota (AC Modernización PFDR).

1. Autenticación en transacciones electrónicas. Aspectos generales

Para garantizar la seguridad de las operaciones electrónicas o transacciones electrónicas, las organizaciones —tanto públicas como privadas— necesitan contar con procedimientos que identifiquen a los usuarios remotos. Este proceso de autenticación electrónica (e-authentication) puede ser implementado en forma segura mediante el uso de una gran variedad de técnicas disponibles que brindan un nivel de confianza sobre la identidad del usuario.

El concepto de "autenticación" se refiere a la verificación de la autenticidad de las identificaciones realizadas o solicitadas por una persona

física o entidad, o sobre datos tales como un mensaje u otros medios de transmisión electrónica.

El proceso de autenticación es el segundo de dos etapas que comprenden:

1. la presentación de una identificación ante el sistema de seguridad y

2. la presentación o generación de información que corrobora la relación entre la entidad y el identificado (ejemplo: me identifico con CUIT y me autentico con clave fiscal para operar con la plataforma de Trámites a Distancia —TAD—[1]).

La Guía de Autenticación Electrónica para Agencias Federales del Gobierno de Estados Unidos define a la autenticación electrónica como "el proceso de establecer confianza en las identidades de los usuarios presentadas electrónicamente ante un sistema de información" (Instituto Nacional de Normas y Tecnología —NIST—, abril de 2006). La autenticación electrónica presenta un desafío tecnológico cuando este proceso involucra la autenticación remota de personas individuales sobre una red informática. Podríamos decir entonces que se entiende por autenticación al proceso mediante el cual se establece un grado de confianza en una afirmación.

2. Autenticación en línea. Marco de confianza

Para entender el desafío de la autenticación en línea, es necesario apreciar las fuentes de confianza en las cuales descansa el entorno comercial actual.

La gente no realiza negocios con personas en las que no confía. Pero esta confianza comercial no es materia de fe, regulación o tecnología, sino que es el resultado de la administración de una relación.

El marco de seguridad y de confianza del nuevo entorno electrónico se compone de distintos aspectos presentes en una situación dada:

1. Entorno jurídico seguro y adecuado: que existan leyes que reconozcan el valor legal de las transacciones electrónicas.

[1] Plataforma de trámites a distancia creada por el decreto N.º 1063/16 del Ministerio de Modernización de la Nación.

2. Entorno tecnológico seguro y adecuado: que se disponga de herramientas que garanticen la seguridad de la información, la confidencialidad de las comunicaciones, la conservación de los documentos electrónicos y la transmisión íntegra de documentos digitales. Respecto de los sistemas, se requieren políticas de seguridad informática adecuadas, con manuales de procedimientos, asignación de responsabilidades y herramientas que permitan garantizar las condiciones de seguridad necesarias.

3. Entorno administrativo seguro y adecuado: que permita definir con claridad los procedimientos de autenticación, los procedimientos de verificación de la idoneidad de los participantes, el proceso de la transacción en sí misma —por ejemplo, de una licitación electrónica— y las personas competentes para participar en él, así como también las responsabilidades asociadas al procedimiento.

En definitiva, se trata de encontrar qué mecanismos pueden utilizarse para hacer más ágiles los procesos de autenticación electrónica sin pérdida de seguridad.

3. Autenticación biométrica

La biometría aporta elementos para proveer el factor "algo que es": el reconocimiento biométrico se refiere al reconocimiento automático de individuos basado en sus características físicas o conductuales. Los datos biométricos no pueden ser robados ni olvidados ni prestados o perdidos. El fraude de credenciales biométricas requiere de un punto de contacto con el titular legítimo de la credencial y la presencia del impostor. La ventaja fundamental es que esta tecnología impide el repudio de una característica física; nadie puede desconocer que se posee un determinado rasgo biométrico[2].

Otra ventaja de la biometría frente a un esquema PKI[3] es la simplicidad de su uso por parte de los usuarios. Son esquemas de autenticación sencillos para la gente, que no requieren recordar claves complejas ni portar dispositivos de claves privadas. La tecnología es más amigable y no tan costosa ni compleja como los esquemas PKI.[4]

[2] Mercedes Rivolta, "Biometría y autenticación digital", capítulo IV del libro *Biometrías*.
[3] Public Key Infrastructure.
[4] Rivolta, "Biometría y autenticación digital: firma electrónica segura o firma digital", 2004.

Desde la perspectiva del efecto jurídico de la autenticación electrónica mediante biometría, debemos considerar que, al ser considerada una firma electrónica, esta forma de autenticación permite dar validez legal a transacciones que se realicen mediante un sistema informático[5].

Esto prueba de qué manera la identificación biométrica puede cumplir un rol complementario con otras tecnologías como PKI, o bien tener un rol propio en la identificación de personas.[6]

A la luz de los avances tecnológicos, el mercado define los mecanismos más seguros y confiables, promoviendo la libre competencia en materia de alternativas y productos de identificación electrónica. Al mismo tiempo, este fenómeno tecnológico es acompañado con las normativas dictadas al respecto por el Banco Central de la República Argentina (BCRA) y con los proyectos desarrollados por el Estado, los cuales se explicarán a continuación.

4. Mecanismo de autenticación: firma digital

La iniciativa de firma digital nace en el seno del Estado nacional en el año 2001 y se origina en el sector público. Sin embargo, su verdadera puesta en marcha se produce con la creación de la Infraestructura de Firma Digital de la República Argentina (IFD-RA), con la DA 6/07.[7]

Es innegable la permeabilidad que la firma digital ha tenido dentro del sector público nacional, entendiéndose por tal el comprendido por todo el sector público nacional conforme lo determina el artículo 8 de la Ley N.º 24.156.

---

[5] La biometría nos permite probar con certeza la autoría de un documento electrónico, pero por sí sola no sirve para probar la integridad o inalterabilidad de un documento electrónico. De allí que se la utilice junto con algún otro método de encriptado del documento.

[6] La resolución UIF N.º 30/217 permite la identificación de clientes mediante el documento original de identidad, el que podrá ser exhibido de manera electrónica o a través de medios digitales acreditados que garanticen seguridad y confianza tecnológica y jurídica, en cuyo caso deberán conservarse las evidencias correspondientes.

[7] Con anterioridad a 2006 en realidad no existía la firma digital, ya que no había ningún certificador licenciado. De allí que por decreto se le haya atribuido a la firma asociada a los certificados emitidos por la ONTI (Oficina Nacional de Tecnologías de la Información) el efecto legal de firma digital. Luego, al aprobarse la DA N.º 6/07, se procedió a regularizar esta situación con el licenciamiento de la ONTI.

Repitiendo conceptos por todos conocidos, nuestro decreto reglamentario de la ley de firma digital contempla tres sistemas de comprobación de autoría e integridad: firma electrónica, firma electrónica basada en certificados emitidos por certificadores no licenciados y firma digital basada en certificados emitidos por un certificador licenciado dentro de la IFD-RA.[8]Esta última es la única firma que —jurídicamente hablando— equivale a una firma manuscrita con beneficios probatorios, incluso mayores que esta firma manuscrita, ya que goza de la presunción de autoría e integridad establecida en los artículos 7 y 8 de la Ley N.º 25.506.

Estas son las características que debe reunir una firma digital para ser tal conforme nuestro marco normativo:

- que la firma se vincule con un documento digital;
- que dicha vinculación se realice mediante la aplicación de un procedimiento matemático que requiera información de exclusivo conocimiento del firmante;
- que dicha información se encuentre bajo el absoluto control del firmante;
- que la firma digital pueda ser verificada por terceras partes;
- que dicha verificación permita identificar al firmante;
- que dicha verificación posibilite detectar posibles alteraciones del documento digital posterior a su firma;
- que haya sido expedida por un certificador licenciado dentro de la IFD-RA.

La ley argentina reconoce la validez jurídica tanto de la firma electrónica como de la firma digital. Se entiende por firma electrónica a todo aquel mecanismo de autenticación que no cumpla con el ciento por ciento de los requerimientos de la ley para la firma digital. En este sentido, pueden ser consideradas firmas electrónicas tanto las claves compartidas (criptografía simétrica), tecnología de clave pública cuyos certificados no fueron emitidos por un certificador licenciado, o bien cualquier mecanismo de autenticación que no cumpla con los requisitos de la ley de firma digital, por ejemplo el PIN personal, el nombre escrito al final de

[8] Artículo 1 del decreto reglamentario N.º 2628/02.

un correo electrónico,[9] una palabra clave utilizada para acceder a la banca electrónica, una pregunta y respuesta para autenticarse, pulsar el botón "ACEPTAR" en una aplicación web.[10] La Ley N.º 25. 506 define las características de la IFD-RA, pero la normativa nada dice respecto de la firma electrónica, la cual se define por exclusión.

Ahora bien, los altos requisitos exigidos a los certificadores que desean adquirir el carácter de licenciados y la circunstancia de que dentro del esquema de firma digital solo se admite la identificación presencial del suscriptor[11] produjeron como consecuencia el desarrollo y la aplicación en el sector privado de la nunca reglamentada firma electrónica.

Veamos a continuación cómo, pese a la existencia del controvertido artículo 288 del nuevo Código Civil y Comercial de la Nación,[12] los mecanismos de identificación y autenticación utilizados por el sector privado han contribuido al incremento de la aplicación de firma electrónica en sus distintas variantes.

5. Utilización de tecnologías de identificación y autenticación en el sector financiero

Dada la aparición de nuevas entidades que operan de forma exclusivamente móvil, y los acuerdos existentes entre las empresas fintech[13] con los nuevos bancos, podríamos decir que estamos ante una nueva economía que gira alrededor de Internet, donde los métodos de autenticación utilizados por estos nuevos actores requieren de una implementación sencilla a los fines de su usabilidad por el usuario, usuario que opera indistintamente tanto por home banking como por telefonía celular.

---

[9] Ver fallo de la Cámara Nacional de Apelaciones en lo Comercial "Skillmedia SRL c/ Estudio ML SA s/ordinario", causa 36208/2015.

[10] La Ley Federal de Estados Unidos sobre firma electrónica, la "eSign", define la firma electrónica como todo símbolo o proceso, adjunto o lógicamente asociado con un contrato o archivo electrónico y ejecutado o adoptado por una persona con la intención de firmar un archivo.

[11] Requisitos para ser certificador licenciado, ver resolución N.º 399 E/2016 del Ministerio de Modernización.

[12] El artículo 288 del CCyCN dice: "[…] 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".

[13] Plataformas tecnológicas que facilitan las operaciones y servicios financieros.

Estas empresas cuentan con el aval explícito del gobierno, que busca limitar el uso del dinero físico y expandir la "inclusión financiera" y la bancarización. La exigencia actual de acceso remoto a servicios financieros y otras actividades en forma no presencial —lo que se conoce como validación de identidad en procesos de onboarding[14]— demanda una regulación legal que permita a la industria financiera alinearse con las mejores prácticas globales.

Así lo entendió el Banco Central, el cual no tardó en adecuarse a esta situación y procedió a dictar la Comunicación BCRA A 6059,[15] la que permite la apertura de una caja de ahorro a distancia, en forma no presencial, de tal manera que las entidades financieras pueden ofrecer un canal digital que cumpla con los estándares del BCRA, para lo cual deben aplicar mecanismos que permitan identificar al cliente y asegurar la autenticidad de la información recibida, posibilitando su cruzamiento con la información disponible en las bases de datos públicas y privadas.

Asimismo, el dictado de las comunicaciones del BCRAA 6068 y A 6072 permite la utilización de soportes digitales por parte de las entidades financieras: establece que estas pueden instrumentar operaciones bancarias en cualquier soporte electrónico en la medida en que dicho

[14] El "onboarding digital" se refiere a la apertura remota de productos y servicios financieros mediante la identificación y registro de clientes a través de una videoconferencia que se basa en el uso de la tecnología biométrica para reconocimiento óptico y facial, así como la captura de documentos de identificación oficial. Todas las secuencias de video se guardan y sirven para una adecuada validación de los datos del solicitante y con ello facilitar el acceso al servicio o producto que requiere contratar.

[15] La Comunicación N.º 6059 dice: "Cuando las entidades financieras admitan que personas humanas que no sean clientes gestionen la apertura de cajas de ahorros a través de medios electrónicos y/o de comunicación que les permitan suplir su presencia física en la casa operativa de la entidad, deberán asegurarse de que tales medios les permitan dar total cumplimiento a la normativa en materia de prevención del lavado de activos y del financiamiento del terrorismo —especialmente en lo referido a la identificación y conocimiento del cliente—, así como a las restantes disposiciones que sean de aplicación. Para ello, deberán adoptar procedimientos, tecnologías y controles que: (i) permitan verificar la identidad del solicitante y la autenticidad de los datos recibidos —los cuales podrán incluir el requerimiento de información de bases de datos públicas y/o privadas para su comparación con los datos recibidos del solicitante—; (ii) aseguren el cumplimiento de las disposiciones en materia de canales electrónicos y las relacionadas con la conservación, integridad, autenticidad y confidencialidad de las informaciones y documentos empleados, protegiéndolos contra su alteración o destrucción así como del acceso o uso indebidos.

soporte sea inalterable y se pueda probar la autoría y autenticidad de la operación.[16]

Los métodos de identificación y de autenticación que actualmente utilizan las entidades financieras son:

- uso de la firma electrónica/digital indistintamente para fines de firma, autenticación y/o cifrado de documentos electrónicos;
- doble factor de autenticación;
- token de seguridad;
- tarjeta de coordenadas;
- certificados de firma digital (emitidos por entes no licenciados en la mayoría de los casos);
- biometría, que puede ser de dos tipos:
  1. fisiológica: huella digital, iris y retina, reconocimiento facial, geometría de mano, etc.;
  2. de comportamiento: firma, voz, comportamiento de teclado, etc.
- firma grafométrica: es la que se produce cuando se genera un formulario digital y el usuario impacta su firma electrónica desde una tablet, lo cual permite reducir la cantidad de firmas y papelería impresa, como así también el tiempo de la gestión;
- captura de firma manuscrita en tablet con almacenamiento de datos biométricos. En este caso, los datos biométricos se almacenan junto con el documento electrónico y se firma la huella del documento electrónicamente (uso de criptografía asimétrica).

Merece un capítulo aparte reflexionar respecto del uso de la firma en tablets con almacenamiento de los datos capturados y su validez legal. En este caso no sería posible vincular la firma que se realiza de manera única con los datos que se pretenden firmar, puesto que el medio por el que se realiza este tipo de firma (la propia tablet) no se mantiene bajo el exclusivo control del firmante. Por lo que no nos encontramos en el terreno de la firma digital pero sí podríamos considerarla como firma electrónica puesto que su inserciónse lleva a cabo de manera electró-

[16] Ante la falta de regulación al respecto por parte del CCyCN, el BCRA permite la digitalización de la firma ológrafa en los documentos electrónicos, la que debe cumplir con los requisitos biométricos indicados por el estándar ISO IEC 19.794-7, debiendo ser conservadas las firmas mediante encriptación para garantizar la integridad y evitar el reemplazo del documento".

nica (la digitalización de la rúbrica en la tableta) y tiene como función identificar al firmante respecto a unos datos asociados o consignados a la mencionada firma. Dicho de otra manera, la firma realizada mediante tablet se puede considerar una firma electrónica desde el punto de vista jurídico ya que no se encuentra inmediatamente vinculada al contenido del documento.

Todos estos tipos de medios de identificación y de autenticación nos permiten identificar al firmante, en algunos casos con mayor robustez que en otros, pero sirven indudablemente para probar la autoría y la integridad de un documento, ya que la autenticidad de la firma se puede probar por cualquier medio y la valoración probatoria del instrumento o documento electrónico se realizará conforme lo determina el artículo 319 del Código Civil y Comercial de la Nación[17].

6. El proyecto de "Identificación digital única"

El Ministerio de Modernización (a través de la Secretaría de Gestión e Innovación Pública), junto con el Ministerio del Interior, con el objetivo de satisfacer el requerimiento de identificación y validación de identidad a distancia, crea el llamado proyecto de "Identidad digital única". Su objetivo es brindar desde el Estado una solución de autenticación biométrica a las empresas para lograr:

- el desarrollo del e-government;
- la evolución y el fortalecimiento de la economía digital de Argentina;
- la simplificación y oferta de más y mejores servicios públicos y privados al ciudadano.

En la Argentina la identidad legal está basada en el Documento Nacional de Identidad (DNI) emitido por el Registro Nacional de las Perso-

[17] Ver Cámara Nacional de Apelaciones en lo Comercial "Skill media SRL c/ Estudio ML SA s/ ordinario", causa 36208/2015. El dictamen pericial avalado por la sentencia de segunda instancia establece: "[…] se prueba la existencia de los correos entrantes y salientes por una de las partes lo que es prueba suficiente para admitir los mails presentados por la otra parte y condenar a la actora". Desde un punto de vista jurídico, un mail es un documento electrónico firmado de manera electrónica ya que contiene datos vinculados lógicamente con el mensaje que el autor utiliza habitualmente para identificarse. Para que la firma electrónica tenga efectos, o bien el autor reconoce el documento, o bien la persona que quiere hacerlo valer prueba que es de su autoría.

nas (Renaper). Este documento es obligatorio, está disponible para todos los ciudadanos y es universalmente aceptado. Actualmente existen alrededor de 44 millones de ciudadanos enrolados en el Renaper con foto de rostro, huella dactilar y DNI emitido. Con esta explicación se justifica que este proyecto sea liderado por el Estado.

En líneas generales, se basa en una aplicación desarrollada por el Ministerio de Modernización que tiene como objetivo validar la identidad de las personas físicas a distancia, cotejando los datos ingresados contra la base de datos del Renaper.

En una primera etapa, el servicio de identificación remota ofrece a las empresas los siguientes servicios: autenticación y vigencia del DNI; reconocimiento facial, con prueba de vida; geolocalización; identificación de dispositivos; reportes/métricas.

En una segunda etapa se implementarán otros métodos de validación biométrica, tales como voz y huellas.

Para que las empresas puedan autorizar el llamado "onboarding digital", o bien realizar transacciones a distancia, deberían suministrar a dicha herramienta tecnológica o software desarrollado por el Estado los datos públicos del solicitante (por ejemplo, los datos de su DNI, foto de rostro, huella dactilar, sexo de la persona, etc.). Los datos de salida se basan en las coincidencias encontradas y en el puntaje arrojado por el software al realizar el cotejo de los datos.[18]

El servicio ofrecido al Sector Privado consiste en un sistema prepago, el cual se abona conforme al uso o transacciones efectuadas o bien conforme a los acuerdos que se realicen al efecto.

De esta forma el Estado garantiza y valida una identidad, y realiza negocios con las empresas y colegios profesionales.[19]

El objetivo del proyecto de identidad digital es eliminar el fraude y la suplantación de identidad en el proceso de identificación, de allí su utilidad

[18] El rostro es un medio de identificación legalmente obligatorio, en los términos del artículo 9 de la Ley N.º 17.671. La biometría por rostro es un modo de identificación legalmente válido y adaptado a las nuevas tecnologías, tal como se propugna en el artículo 11 de la Ley N.º 11.671 y su reglamentación en el artículo 1 del decreto N.º 1501/09.

[19] Uno de los primeros colegios profesionales que cerraron acuerdo conel Ministerio del Interior y Modernización para acceder a la base de datos del Renaper, a fin de validar identidad, fue el Colegio de Escribanos, que es una autoridad de registro de la ONTI.

y ofrecimiento al sector privado como servicio de software "as a service"[20] en una primera etapa, para evolucionar luego a un sistema "web service"[21].

7. Conclusiones

El Estado siempre sostuvo la validez y la eficacia de la firma digital y de la firma electrónica, no obstante, y con el objeto de simplificar procesos, comienza a aceptar el uso de la firma electrónica y a extender su aplicación como medio de identificación y validación de identidad en caso de acceso remoto a servicios financieros y otras actividades en forma no presencial.

Finalmente, convalida todas las iniciativas del sector privado y regulaciones dictadas por el BCRA mediante el decreto N.º 27/18, el cual en su capítulo XXII, referente a inclusión financiera, establece "[…] que el requisito de la firma del titular quedará satisfecho si se utiliza cualquier método que asegure indubitablemente la exteriorización de la voluntad de las partes y la integridad del instrumento".

El proyecto de identificación digital único basado en la identificación biométrica de las personas físicas se complementa con otra iniciativa del Estado disponible solo para identificación de personas físicas, que se conoce como "firma digital remota", regulada por decreto N.º 892/2017, resolución N.º 121/18 y resolución N.º 13/2018.

8. Firma digital remota

La evolución de las TIC[22] hacia entornos basados en el cloud computing y la movilidad, está cambiando los paradigmas preestablecidos respecto a la firma digital y a la identidad digital, creando a

[20] "Software como un servicio", abreviadamente (del inglés: software as a Service, SaaS), es un modelo de distribución de software en el cual el soporte lógico y los datos que maneja se alojan en servidores de una compañía de tecnologías de la información y la comunicación (TIC), a los que se accede vía Internet desde un cliente.

[21] Web service: significa que distintas aplicaciones de software desarrolladas en lenguajes de programación diferentes, y ejecutadas sobre cualquier plataforma, pueden utilizar los servicios web para intercambiar datos en redes de ordenadores como Internet. La interoperabilidad se consigue mediante la adopción de estándares abiertos.

[22] Empresas que se dedican a las tecnologías de la información y la comunicación.

su vez un abanico de servicios relacionados hasta ahora prácticamente desconocidos.

Conceptos como firma remota, gestión centralizada de claves, firma en movilidad, firma digitalizada, custodia de documentos a largo plazo y los nuevos escenarios creados por el desarrollo de la administración electrónica y sus normas de aplicación, especialmente en lo relativo a la adecuación de los esquemas nacionales de interoperabilidad y seguridad, están haciendo evolucionar los recursos de PKI[23] desde un contexto basado en aplicaciones distribuidas hacia un elemento crítico de infraestructura y el consumo de servicios de firma digital centralizada.

La tecnología en la nube se extiende al campo de la autenticación y por eso se habla de firma "en cloud" o firma en la nube[24]. En realidad hablamos de un software como servicio "as a service" que permite al usuario trabajar con determinadas aplicaciones y programas sin necesidad de instalarlos en su equipo. Así aumenta la usabilidad de la aplicación, a la cual se puede acceder desde cualquier dispositivo.

9. Por qué es necesaria la firma digital remota

Si bien la identificación electrónica parece que está relativamente resuelta, la firma digital supone una barrera en el uso de muchos procedimientos electrónicos que están a disposición de los ciudadanos.

Habitualmente, cuando debemos utilizar firma digital, a los administrados o usuarios se nos plantean problemas como los siguientes:

a) inconvenientes a la hora de gestionar e instalar correctamente el software y/o hardware en algunas situaciones;

b) la firma digital con terminales móviles, como smartphones o tablets, a la fecha de hoy no es muy usada, o la tecnología está poco desarrollada, por lo cual surgen inconvenientes, en especial con la gestión y la instalación de los certificados electrónicos en telefonía móvil, o bien para encontrar lectores de tarjeta criptográficas que sean compatibles con estos dispositivos.

[23] Sigla que identifica a una infraestructura de clave pública.

[24] La tecnología y los sistemas en la nube (cloud computing) están ganando importancia cada día. Sin duda, esta tendencia se extiende al campo de la autenticación, lo que da lugar a la aparición de la firma en cloud.

En el caso de firma digital centralizada o en la nube, el proveedor de servicio (o recomendablemente un tercer actor) será el responsable de la gestión y de la custodia de los certificados de firma. Al realizar la firma, el interesado expresará su voluntad (por ejemplo, con una contraseña y un código OTP[25] generado en el momento y enviado a un dispositivo móvil). En ese instante se desencadenará la firma del documento en el servidor (nube) de tal forma que el certificado electrónico nunca saldrá del servidor custodio. El responsable de la custodia de los certificados debe ser una entidad de confianza que debe cumplir con las garantías de seguridad necesarias. Por esto la firma digital remota, como se explicará a continuación, implica la disponibilidad de los certificados y de los datos de creación de firma en un servidor exclusivo administrado por el Estado y situado en nuestro territorio, conforme a los estándares tecnológicos y operativos de la Infraestructura de Firma Digital que el mismo Ministerio de Modernización establece como autoridad de aplicación de la IFD-RA.

10. Plataforma de firma digital remota

La plataforma de firma digital remota, conforme al decreto N.º 892/2017, va a ser administrada exclusivamente por el Ministerio de Modernización, y suministrada en forma gratuita utilizando los procedimientos de firma y de verificación establecidos por la autoridad de aplicación de la IFD-RA.[26] Por su parte, los certificados de firma digital asociados al uso de firma digital remota serán emitidos por la Autoridad Certificante dependiente del Ministerio de Modernización (AC Modernización PFDR), conforme su política única de certificación.

Conforme surge del texto del decreto antes referido, la plataforma de Firma Digital Remota opera utilizando un sistema técnicamente confiable y seguro acorde a los lineamientos de la Ley N.º 25.506 y respetando los siguientes estándares:

a) resguardar contra la posibilidad de intrusión y/o uso no autorizado;

[25] One Time Password: código de seis dígitos que llega a su celular a través de un mensaje de texto.
[26] El decreto N.º 27/18 reemplaza el artículo 30, inciso b de la Ley N.º 25506, y establece que la autoridad de aplicación, que en este caso es el Ministerio de Modernización, determinará los estándares tecnológicos y operativos de la Infraestructura de Firma Digital.

b) asegurar la disponibilidad, confiabilidad, confidencialidad y correcto funcionamiento;

c) ser apto para el desempeño de sus funciones específicas;

d) cumplir las normas de seguridad apropiadas, acorde a estándares internacionales en la materia;

e) cumplir con los estándares técnicos y de auditoría establecidos por la autoridad de aplicación de la Ley N.º 25.506.

11. Características de nuestra IFD-RA

En la Argentina, la Infraestructura de Firma Digital descansa sobre la confidencialidad de la clave privada del firmante. Esta clave solo puede ser generada, almacenada y utilizada por su titular (generalmente se almacena en un dispositivo criptográfico homologado por la autoridad de aplicación). El certificador no tiene copia de dicha clave. El usuario tiene que tener el control absoluto de sus datos de creación de firma y no puede compartirlos, por lo que debe impedir su divulgación. Ni el certificador ni las autoridades de registro pueden tomar conocimiento o acceder a dichas claves.

En líneas generales, el certificador no puede generar los datos de creación de firma del suscriptor, por lo que al no tener copia de la clave privada del suscriptor, en caso de que dicha clave se pierda, nunca se podrá restaurar; no quedará otra alternativa más que proceder a la revocación del certificado correspondiente.

Asimismo, conforme la resolución N.º 333/16, que reglamenta toda la actividad de los certificadores licenciados, se exige que toda la infraestructura tecnológica que soporta los servicios del certificador se encuentre en la Argentina y bajo la exclusiva responsabilidad del certificador, por lo que nuestro sistema no solo no se permite al certificador crear, tomar conocimiento, acceder a los datos de creación de firma, duplicarlos o bien almacenarlos en sus propios servidores, sino que tampoco se permite almacenarlos en servidores propios o de terceros situados en el exterior.

Solo apelamos a la figura de la gestión de datos en nombre de otro para el caso de solicitud de certificados de personas jurídicas; aquel que actúa como gestor asume la responsabilidad por la custodia de dichos datos de creación de firma.

Como autoridad de aplicación, el Ministerio de Modernización prohíbe a los certificadores licenciados la posibilidad de emitir certificados en la nube, puesto que entiende que sería imposible auditar y supervisar una infraestructura tecnológica que permita disponibilizar este tipo de certificados en servidores propios o de terceros.

Por ese motivo este proyecto se puso en marcha en forma exclusiva por el Ministerio de Modernización, organismo que a dichos fines y efectos ha creado una nueva autoridad certificante (AC Modernización PFDR), y queda a voluntad del suscriptor o titular de los datos consentir o no dicha modalidad de uso.

Sin duda la firma digital remota, como herramienta tecnológica expedida por el Estado en forma gratuita, ha mostrado a la fecha un alto nivel de aceptación en el sector privado que presta servicios financieros, como complemento necesario del sistema de identificación biométrica o proyecto de identificación digital ya descripto.

12. Política de Certificación de la Autoridad Certificante que utiliza la plataforma de firma digital remota administrada por la Dirección Nacional de Gestión de la Información y de Soporte de la Secretaría de Modernización Administrativa

La Autoridad Certificante del Ministerio de Modernización que utiliza la Plataforma de Firma Digital Remota (AC Modernización PFDR), que se encuentra recientemente licenciada mediante la resolución N.º 13/2018, establece que los solicitantes o suscriptores de certificados, en líneas generales, deberán contar con un teléfono móvil "inteligente" e instalar una aplicación OTP para que, junto con otros factores de autenticación, puedan lograr firmar en forma digital desde cualquier dispositivo, eliminando las barreras de los dispositivos comúnmente utilizados.

Los suscriptores de esta política de certificación son las personas físicas[27] humanas que requieran un certificado digital para firmar digitalmente cualquier documento o transacción, pudiendo ser utilizados para

[27] No se entiende por qué la normativa no dice "personas físicas" en vez de "personas humanas". También hay que resaltar que sólo se emiten certificados de personas físicas. Ni la AC de Modernización ni la AC ONTI emiten certificados de personas jurídicas.

cualquier uso o aplicación, como así también para autenticación o cifrado. También podrán ser suscriptores los funcionarios, agentes o personas que se desempeñen en el sector público y los particulares que interactúen con las aplicaciones del Estado.

13. Identificación y autenticación de la Autoridad Certificante de Modernización PFDR

El proceso de validación de identidad del suscriptor es presencial. Para poder llevarlo a cabo, se aumentaron los requisitos a cumplir por las autoridades de registro del sector privado mediante el dictado de la siguiente normativa: se procedió a la modificación del artículo 36 del decreto N.º 2628/02, que establece que los certificadores licenciados de organismos públicos podrán constituir autoridades de registro pertenecientes al sector privado, previa autorización de la Secretaría de Modernización Administrativa del Ministerio de Modernización. Por otro lado, la Secretaría de Modernización Administrativa dictó la resolución N.º 116-E/201, la cual impone más restricciones a los procedimientos de identificación llevados a cabo por los certificadores licenciados, los que aparte de tener que cumplir con todos los requisitos impuestos por el decreto N.º 399/17, deberán identificar a los suscriptores —sin perjuicio de lo que establezca la política de certificación al respecto—, capturando fotografía digital del rostro y la huella dactilar de los solicitantes y suscriptores de certificados de firma digital, almacenando la fotografía digital en formato JPEG y la imagen y la minucia de la huella dactilar de acuerdo con el estándar ISO/IEC 19794-2.

14. Procedimiento de identificación y autenticación

1. Presentación del solicitante ante la autoridad de registro.
2. Registración de datos del solicitante por la AR y entrega al solicitante de contraseña temporal impresa.
3. Verificación de dirección de correo electrónico del solicitante.
4. Confirmación de datos por solicitante.
5. Creación de segundo factor de autenticación.

La aplicación de la autoridad certificante envía al usuario o suscriptor un código OTP Luego el usuario debe escanear el código en su celular o dispositivo móvil e ingresar el OTP asociado a su cuenta de usuario. A continuación el usuario debe crear un segundo factor de autenticación (PIN de su clave privada) y, como paso final, debe efectuar la solicitud de su certificado.

El suscriptor debe resguardar los factores de autenticación creados (PIN y contraseña OTP) que permiten utilizar la clave privada alojada en la plataforma. La plataforma es la encargada de generar, almacenar y custodiar las claves privadas de los suscriptores que interactúan con la AC. Si bien entendemos que la política única de certificación de la nueva AC de Modernización no se ajusta a los requerimientos que la normativa que rige la IFD-RA exige a los certificadores licenciados conforme a lo hasta aquí expuesto, entiendo que sí se adapta a las exigencias tecnológicas de la nueva economía y a las necesidades de negocios del sector privado, por lo que se espera que su implementación sea realmente exitosa.

15. Recomendación de la Comisión de la Comunidad Europea relativa a aspectos jurídicos del intercambio electrónico de datos

La Comunidad Europea promueve la firma "en cloud" para crear un mercado digital único europeo (reconocimiento recíproco de todos los certificados de los países integrantes de la CE) y, básicamente, para agilizar el comercio electrónico y el uso de las aplicaciones móviles.[28]

Solo los prestadores de servicios cualificados (reconocidos o licenciados, sería en nuestra terminología) podrán prestar servicios de firma "en cloud" y serán distinguidos con una etiqueta de confianza.

La normativa española inicialmente prohibía al proveedor de servicios de certificación copiar los datos de creación de firma y almacenarlos. No obstante, la ley de firma electrónica española[29] se ha adaptado a la recomendación de la Comisión Europea al establecer: "[…] los prestadoras

[28] Ver reglamento IDAS de la Unión Europea sobre identificación electrónica y servicios de confianza 910/204 (etiqueta de confianza para prestadores cualificados).

[29] Ver disposición final cuarta. Modificación de la Ley N.º 59/2003, de 19 de diciembre, de firma electrónica.

de servicios de certificación no podrán almacenar ni copiar, por sí o a través de un tercero, los datos de creación de firma de la persona a la que hayan prestado sus servicios, salvo en caso de su gestión en nombre del firmante. En este caso, se aplicarán los procedimientos y mecanismos técnicos y organizativos adecuados para garantizar que el firmante controle de modo exclusivo el uso de sus datos de creación de firma. Solo los prestadores de servicios de certificación que expidan certificados reconocidos podrán gestionar los datos de creación de firma electrónica en nombre del firmante […]".

En síntesis, la movilidad está cambiando los paradigmas preestablecidos de firma digital e identidad digital, lo cual requiere la adaptación de los esquemas nacionales de interoperabilidad y seguridad, evolucionando hacia esquemas que permitan una infraestructura de consumo de servicios de firma digital centralizada. Esperamos que en un futuro la Argentina regule detalladamente la prestación de este tipo de servicios por parte de los certificadores licenciados, permitiendo así el desarrollo de la firma digital por parte del sector privado conforme a las nuevas tecnologías y demandas de la sociedad de la información.

16. Los certificados de atributos: su problemática

La AC ONTI y la AC de Modernización (PFDR) no emiten certificados de atributos ni certificados para personas jurídicas. Solo se emiten certificados para personas físicas y aplicaciones.

La autoridad de aplicación solo autoriza la emisión de certificados de personas físicas porque entiende que la función de unir la identidad estática de una persona a una determinada clave pública es un riesgo gestionable, pero la función de la autoridad certificante de unir atributos dinámicos de una persona a un par de claves públicas (que es lo que suele suceder en los certificados emitidos para personas jurídicas) es más complicada de gestionar eficazmente, sobre todo cuando no se trabaja conectado a la base de datos de otros organismos públicos.

En síntesis, a la autoridad de certificación se le hace difícil de controlar el cambio de información dinámica de una persona jurídica, lo cual le generaría responsabilidad frente a los terceros usuarios que confían en la apariencia registral y, por ende, en la validez de dicha firma.

Cuando ese cambio de atributo dinámico no es informado a su debido tiempo, se mantiene activo un certificado que debería haber sido revocado de inmediato, por lo tanto, al confiar solamente en la información proporcionada por el solicitante, la autoridad certificante podría estar emitiendo o considerando activo un certificado inválido. Consideremos el caso de un certificado de atributos en el que consta la condición de administrador social del titular. Si se produce el cese del administrador en su cargo, puede ocurrir que el cese se haya inscripto en el registro pero todavía no se haya revocado el certificado. En este caso existe una presunción de conocimiento por parte del tercero usuario, siempre que no se aprecie la mala fe del titular del certificado, quien puede no haber solicitado la revocación deliberadamente para actuar en forma fraudulenta.

Desde el punto de vista de la responsabilidad y distribución del riesgo, el sistema de certificados tiene sus propias peculiaridades, a diferencia del mercado de las tarjetas de crédito, dado que el sistema de certificados tiene un alto grado de imprevisibilidad. En el caso de las tarjetas de crédito, existe un límite máximo de autorización, que representa el riesgo asumido por la entidad emisora y por el titular en caso de pérdida o sustracción. En cambio, cuando se expide un certificado, este puede adjuntarse a varias transacciones cuyo monto total, la mayoría de las veces, sería imprevisible.

Con el fin de evitar responsabilidad por parte de la AC, lo ideal sería que cuando se emita un certificado de atributos, tal circunstancia conste en el registro correspondiente, de tal forma que cuando se quiera dar de baja el atributo en forma registral, previamente se exija la revocación del certificado. De esta forma no existiría un certificado que genere una apariencia extrarregistral distinta de la registral.[30]

Los certificados de personas jurídicas fueron erradicados por la actual autoridad de aplicación de la IFD-RA, pese a lo establecido en el artículo 37 de la resolución N.º 399-e/2016,[31] como así también los llamados

[30] Apollònia Martínez Nadal, *Comercio electrónico*, *firma digital* y *autoridades de certificación*.

[31] El artículo 37 dice: "Las personas jurídicas podrán solicitar certificados digitales a través de sus representantes legales o apoderados con poder suficiente a dichos efectos, quienes tendrán la responsabilidad de la custodia de los datos de creación de firma asociados y cuyos datos de identi-

"certificados de competencia" que establecía la derogada decisión administrativa N.º 927/2014.

Entiendo que esta es la explicación por la cual entiendo que certificados de competencia y los Colegios profesionales como certificadores licenciados, quedaron excluidos de la IFD-RA, conforme así lo expresa el nuevo decreto N.º 27/18.

17. Hacia una firma electrónica segura

Según lo expuesto, en el sector privado las relaciones electrónicas se desenvuelven conforme al principio de proporcionalidad, por lo que de acuerdo con la naturaleza de la transacción a realizar se exigirán las garantías y las medidas de seguridad adecuadas.

La firma electrónica segura es avalada por el Estado a través del dictado del decreto N.º 927/18.[32] El hecho de que se espera que este decreto sea ratificado por ley no hace más que convalidar la política de inclusión financiera llevada a cabo por el BCRA, estableciendo los supuestos en los

ficación deberán ser incluidos en el certificado. Los certificados de aplicación serán solicitados por las personas jurídicas para sus aplicaciones informáticas o servidores, a través de sus representantes legales o apoderados con poder suficiente a dichos efectos. La constancia de la identificación de la persona física responsable de la custodia de los datos de creación de firma asociados a cada certificado digital, deberá ser conservada por el certificador licenciado, como información de respaldo de la emisión del certificado.

[32] Finalmente llega la regulación de la firma electrónica al establecer que en el contrato de emisión de tarjeta de crédito se podrá llevar a cabo en forma electrónica, y se fija que el requisito de la firma del titular y de personal apoderado de la empresa emisora quedará satisfecho si se utiliza cualquier método que asegure indubitablemente la exteriorización de la voluntad de las partes y la integridad del instrumento. En el caso del cheque, el BCRA, como autoridad de aplicación, reglamentará las fórmulas del cheque y decidirá sobre todo lo conducente a la prestación de un eficaz servicio de cheque, incluyendo la forma documental o electrónica de la registración, rechazo y solución de problemas meramente formales de los cheques. También determinará todo lo atinente al sistema de firma del librador, y se podrá utilizar sistemas electrónicos o de reproducción cuando expresamente lo autorice el Banco Central de la República Argentina. En materia de letra de cambio se establece que si el documento fue generado electrónicamente, la aceptación debe hacerse en la letra de cambio y expresarse con la palabra "aceptada", "vista" u otra equivalente y firmada por el girado. Al poderse utilizar cualquier método que asegure indubitablemente la exteriorización de la voluntad del girado y la integridad del instrumento, lo mismo se establece respecto de la firma del avalista en la letra de cambio y para la aceptación por intervención en la letra de cambio. Regula el pagaré electrónico y también establece que la firma del suscriptor quedará satisfecha si se utiliza cualquier método que asegure indubitablemente la exteriorización de la voluntad del suscriptor y la integridad del instrumento.

que se puede utilizar una firma electrónica robusta que asegure autoría e integridad del documento.

La referida normativa reconoce y reglamenta el uso de la firma electrónica y del documento electrónico, e incluso hace viable la llamada desmaterialización de los títulos valores cartulares,[33] estableciendo la posibilidad de emitir títulos valores electrónicos y firmarlos electrónicamente conforme lo establezca el BCRA como autoridad de aplicación, respondiendo así a una demanda sostenida por el sector privado.[34]

Finalmente, es de esperar que las medidas —detalladas anteriormente— tomadas por el Ministerio de Modernización, en su carácter de autoridad de aplicación de la IFD-RA, puedan ser sostenidas técnica y operativamente para lograr la articulación cotidiana y práctica del ciudadano con la tecnología de firma digital, circunstancia que me parece que no depende solo del dictado de normas técnicas difíciles de comprender sino también de la capacidad de capacitar y educar a la ciudadanía.

[33] Ver artículo 1836 del Código Civil y Comercial de la Nación.

[34] El sector privado exigía la necesidad de desmaterializar los títulos valores y emitirlos como títulos valores electrónicos conforme lo establece el referido artículo 1836 del nuevo Código Civil y Comercial. El decreto N.º 27/18 señala la posibilidad de generar electrónicamente títulos valores electrónicos. Este título electrónico representativo de derechos va a requerir de entidades autorizadas por el BCRA para llevar a cabo la anotación electrónica de los distintos actos cambiarios llevados a cabo sobre el título valor. Esta función podría ser realizada tranquilamente por terceros de confianza o certificadores licenciados sin perjuicio de otras entidades, como cajas de compensación, o bien autoridades financieras autorizadas por el BCRA.

Firma digital y tutela judicial efectiva: medidas cautelares en base a instrumentos electrónicos privados

por Ariel E. Provenzani Casares

Resumen: el autor analiza como plantear medidas cautelares en base a documentos electrónicos privados firmados digitalmente.

Abstract: the author studies how to request injunctions in court with electronic document and digital signatures.

Palabras clave: firma digital – documento electrónico – cautelar – proceso judicial.

Sabido es que, en multiplicidad de casos, la posibilidad de obtener un pronunciamiento judicial *efectivo* (es decir, *realizable* o *útil*) depende de la traba oportuna de una medida cautelar por parte del actor, quien, para obtenerla, debe acudir al proceso cautelar; proceso accesorio de otro principal en el que habrá de discutir con el demandado, frente al juez y con la profundidad necesaria, los méritos de su pretensión.

Ya en 1935, en su clásico estudio sobre las medidas cautelares, Piero Calamandrei señalaba que "Las providencias cautelares representan una conciliación entre las dos exigencias, frecuentemente opuestas, de la justicia: la de celeridad y la de la ponderación; entre hacer las cosas pronto pero mal, y hacerlas bien pero tarde, las providencias cautelares tienden, ante todo, a hacerlas pronto, dejando que el problema de bien y mal, esto es, de la justicia intrínseca de la providencia, se resuelva más tarde, con la necesaria ponderación, en las reposadas formas del proceso ordinario. Permiten de este modo al proceso ordinario funcionar con calma, en cuanto aseguran preventivamente los medios idóneos para hacer que la providencia, al ser dictada, pueda tener la misma eficacia y el mismo rendimiento *práctico* que tendría si se hubiese dictado inmediatamente"[1].

[1] *Introducción al estudio sistemático de las providencias cautelares*, Librería El Foro, impresión de 1997, pp. 43 y 44.

De modo tal y desde aquel punto de vista, "Cautelar se llama al proceso cuando, en vez de ser autónomo, sirve para garantizar (constituye una cautela para) el buen fin de otro proceso (definitivo)",[2] "El proceso cautelar tiende a impedir que el derecho cuyo reconocimiento se pretende obtener a través de un proceso (de conocimiento o de ejecución) pierda su virtualidad o eficacia durante el tiempo que transcurre entre su iniciación y el pronunciamiento de la sentencia que le pone fin (desaparición de los bienes del presunto deudor, o modificación de la situación de hecho existente al tiempo de deducirse la pretensión). La característica fundamental de este tipo de procesos consiste en *que carecen de autonomía*, pues su finalidad se reduce a asegurar el resultado práctico de la sentencia que debe recaer en otro proceso"[3].

También son conocidos los extremos objetivos que debe abastecer quien solicite una medida cautelar: *verosimilitud del derecho* y *peligro en la demora*, recaudos que "deben evaluarse en forma armónica, de manera que a mayor verosimilitud del derecho no cabe ser tan exigente en la gravedad e inminencia del daño"[4]. Ello no implica, claro está, que el

[2] Carnelutti, Francesco: *Instituciones del Proceso Civil*, Librería El Foro, 1997, vol. I, p. 86.

[3] Palacio, Lino Enrique: *Manual…*, vigésima edición, reimpresión, Abeledo Perrot, 2011, p. 64. Insisto: desde el punto de vista elegido pues, como señalan Arazi y Kaminker, "se ha ampliado el objeto de estas medidas e, incluso, sus principios y caracteres son aplicables a otros supuestos, como sucede con el trámite de los procesos urgentes" (*Medidas cautelares*, tercera edición, Roland Arazi (dir.), Astrea, 2007, p. 1).

[4] Arazi y Kaminker, *op. cit.*, nota 3, p. 4. En el mismo sentido, Cámara Nacional de Apelaciones en lo Comercial Sala A, "Laboratorios Andrómaco SAICI c/ El Cabildo Cía. Argentina de Seguros Generales SA s/ ord. s/ inc. de apelación s/ CPR 250" (21/4/93), entre muchos: "verosimilitud del derecho y el peligro en la demora son dos recaudos genéricos de toda medida cautelar que debe evaluarse en forma armónica. Así que, a mayor verosimilitud del derecho no cabe ser tan exigente en la gravedad e inminencia del daño y viceversa, cuando existe el riesgo de un daño extremo e irreparable, el rigor acerca del *fumus bonis iuris* se puede atemperar". La misma sala ha dicho en "Mignone SA c/ Colon, Ana s/ ord." (26/6/87) que "Si el embargo preventivo ha sido decretado en atención a la verosimilitud del derecho del actor, que resulta *prima facie* del reconocimiento del demandado del documento que se le atribuye y de los hechos narrados en la demanda al margen de la nulidad opuesta que por el momento no ha sido decretada, no cabe exigir al peticionante de la medida una acreditación más completa de la existencia de peligro en la demora", lo que indica que, en realidad, el peligro en la demora es "un requisito independiente que puede o no actuar en conjunto con el anterior" (Osvaldo A. Gozaíni, *Código Procesal Civil y Comercial de la Nación, Comentado y Anotado*, tercera edición, t. I, p. 940, La Ley, 2011. Este es el caso, v. gr. del artículo 209, inciso 2 del CPCC, que solo requiere verosimilitud del derecho que se pretende asegurar.

actor deba arrimarle al juez elementos que le hagan adquirir plena certeza sobre el punto, sino acreditarlo *sumariamente*, mediante el aporte de pruebas que lo lleven a entender que "existe un alto grado de probabilidad de que la sentencia definitiva que se dicte oportunamente reconocerá el derecho en que funda su pretensión"[5].

Es en este campo donde la firma digital de instrumentos electrónicos privados brinda un importante servicio a la *tutela judicial efectiva*, entendida esta como la *realización oportuna del derecho reclamado por medio del sistema estatal de resolución de conflictos* o, dicho de otro modo, como *efectividad estatal medida por su aptitud para satisfacer, en un plazo razonable, el derecho reclamado por todo aquel que acude a los estrados de la justicia*.

Debo, por supuesto, justificar mi aseveración, a lo que dedicaré los siguientes números de este artículo.

1. Instrumentos privados y medidas cautelares

Como es obvio, el aporte de un instrumento, sea público o privado, constituye un medio idóneo —en el tráfico jurídico moderno sea, tal vez, el medio por excelencia— para demostrar eficazmente la verosimilitud del derecho que pretende asegurarse a través del proceso cautelar.

En cuanto a instrumentos privados, el Código Procesal Civil y Comercial (CPCC) contiene cuando menos dos normas relevantes:

(i) Su artículo 197 dice: "La información sumaria para obtener medidas precautorias podrá ofrecerse acompañando con el escrito en que se solicitaren el interrogatorio de los testigos y la declaración de estos, ajustada a los artículos 440, primera parte, 441 y 443, y firmada por ellos. Los testigos deberán ratificarse en el acto de ser presentado dicho escrito o en primera audiencia. Si no se hubiese adoptado el procedimiento que autoriza el primer párrafo de este artículo, las declaraciones se admitirán sin más trámite, pudiendo el juez encomendarlas al secretario […]".

(ii) Y su artículo 209, incisos 2 y 3, que "Podrá pedir embargo preventivo el acreedor de deuda en dinero o en especie que se hallare en alguna de las condiciones siguientes: […] 2) Que la existencia del crédito

[5] Arazi y Kaminker: op. cit., nota 3, p. 4.

esté demostrada con instrumento público o privado atribuido al deudor, abonada la firma por información sumaria de dos (2) testigos. 3) Que fundándose la acción en un contrato bilateral, se justifique su existencia en la misma forma del inciso anterior, debiendo en este caso probarse además sumariamente el cumplimiento del contrato por parte del actor, salvo que este ofreciese cumplirlo, o que su obligación fuese a plazo".

Estas normas, es evidente, no captan el fenómeno de la *firma digital* que, para el momento en que el CPCC se sancionó, era inimaginable. Por otra parte, la firma digital no consiste en una *grafía*[6] que un testigo pueda reconocer, sino en resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose esta bajo su absoluto control (Ley N.º 25.506, artículo 2). Por otra parte, y en rigor de verdad, nada hay más alejado de los propios principios de la *firma digital* —basada, precisamente, en el secreto de la información utilizada por el firmante para aplicarla— y de la utilidad que brinda para celebrar contratos a distancia por medios informáticos, que su empleo frente a testigos[7].

[6] La firma digital fue creada para facilitar el tráfico jurídico por vías informáticas. Por supuesto, uno o varios testigos podrían presenciar el momento en que alguien aplica la firma digital a un documento electrónico privado, pero ¿cómo podrían estar seguros de que el firmante usó su propia clave privada, por definición *secreta*? ¿Constatando en el mismo acto el certificado digital estampado en él? ¿Y cuál sería el fundamento práctico que justifique rodear a esta facilidad tecnológica de solemnidades medioevales, habida cuenta las presunciones de autoría e integridad que la ley otorga a su empleo? Y aun cuando ello sería concebible (por ejemplo, para la celebración del matrimonio, artículo 418 CCyCN), lo cierto es que el objeto de la testimonial de abono consiste en que el testigo exprese si reconoce la grafía de la firma ológrafa que se le exhibe como perteneciente a determinado sujeto y de razón de sus dichos. Explica Osvaldo Gozaíni (*op. cit.*, nota 4, p. 998) que "La información de abono supone que los testigos reconozcan la firma del obligado o deudor, no que hayan visto [*el acto de*] la firma del documento base de la acción. La exigencia de abonar las firmas de los instrumentos privados, no conlleva necesariamente a la necesidad de que los testigos que producen el acto de reconocimiento hayan presenciado el momento en que los presuntos obligados hayan estampado las firmas que se le atribuyen". A estas nociones tradicionales podría responder la firma ológrafa captada por medios informáticos e impuestas sobre documentos electrónicos (firma mediante lápices ópticos o dígitos) utilizadas por ciertas entidades financieras o de pago e, incluso, dependencias gubernamentales. Sin embargo, este tipo de firma no responde al concepto legal de firma digital en el derecho argentino, aunque sí a la de firma electrónica.

[7] El caso de la nota anterior, es decir, el de la firma ológrafa impuesta sobre documentos electrónicos, parece ser distinto. El propio BCRA las acepta en ciertas condiciones y para ciertos tipos de documentos, pues "Se admiten las firmas ológrafas efectuadas originalmente sobre documentos electrónicos u otras tecnologías similares en la medida que puedan efectuarse sobre aquellas verificaciones periciales que permitan probar su autoría y autenticidad" (ver BCRA, T. O., *Normas*

2. La brecha sustancial-procesal. Posible solución

Por su propia definición y en la mayoría de los casos de uso imaginables, la firma digital queda extramuros de la testimonial de abono que requieren las normas rituales citadas arriba. Nada parece haber en una firma digital que un testigo pueda reconocer, al menos a los fines que establecen aquellas normas y a tenor del significado forense que tradicionalmente se otorga al término *testigo*[8].

Sin embargo, el Código Civil y Comercial de la Nación (CCyCN) otorga plena validez a la instrumentación y firma de actos jurídicos mediante documentos y medios electrónicos (artículos 286, 288 y concs.) y, por su fortaleza como método, la firma digital viene dotada de dos presunciones que, desde el punto de vista probatorio, hacen que el documento electrónico privado firmado digitalmente adquiera un valor similar al de

sobre instrumentación, conservación y reproducción de documentos, punto 1, subpunto 1.2). Claro está que, no siendo consideradas firmas digitales para la legislación argentina, la conclusión parece ser obvia: los documentos privados firmados de este modo no parecen ser los instrumentos privados que exige el artículo 209, incisos 2 y 3 del CPCC, sino instrumentos particulares no firmados. Recuérdese la clasificación del artículo 287 del CCyCN: "Los instrumentos particulares pueden estar firmados o no. Si lo están, se llaman instrumentos privados. Si no lo están, se los denomina instrumentos particulares no firmados; esta categoría comprende todo escrito no firmado, entre otros, los impresos, los registros visuales o auditivos de cosas o hechos y, cualquiera que sea el medio empleado, los registros de la palabra y de información". Cabe preguntarse, sin embargo, si este tipo de instrumentos podrían ser considerados aptos para el otorgamiento de una medida cautelar y qué prueba debería producirse para lograr la sumaria convicción de un juez sobre la autenticidad del instrumento presentado, atento el principio de libertad de formas que campea en el CCyCN (artículos 284 y 1.015) y la amplitud probatoria establecida por su artículo 1.019 ("Los contratos pueden ser probados por todos los medios aptos para llegar a una razonable convicción según las reglas de la sana crítica, y con arreglo a lo que disponen las leyes procesales, excepto disposición legal que establezca un medio especial"). En todo caso, no parece razonable responder este interrogante *a priori* de modo negativo, por la mera clasificación legal de cierto instrumento como "privado no firmado". Laura Rodríguez Prada sostiene que "La prueba testimonial puede suplirse por cualquier otra que incline al sentenciante a presumir que existe el crédito cuya percepción trata de asegurarse a través de la medida cautelar. De otro modo, la norma procesal en cuestión entraría en conflicto con disposiciones del Código Civil relativas a la prueba de los contratos" (*op. cit.*, nota 3, p. 82). En otras palabras, si un instrumento de esta clase puede sostener la plena prueba de un contrato, con más razón debería sostener su prueba sumaria.

[8] El certificador licenciado cumple, en la firma digital, la función de un tercero de confianza encargado de producir y custodiar información relevante sobre la autoría de un documento y su integridad. En este sentido, parece ser un *equivalente funcional* del testigo que concurre al acto, o del escribano que certifica las firmas de sus otorgantes.

los instrumentos públicos o, cuando menos, al de los instrumentos privados con firmas certificadas: se trata de las presunciones de autoría e integridad que consagran los artículos 7 y 8 de la Ley N.º 25.506[9]. De tal modo, concluir que un documento electrónico privado firmado digitalmente es apto para instrumentar y probar con plenitud un acto jurídico pero, a su vez, y por un mero imperativo ritual, no lo es para acreditar la verosimilitud del derecho a fines cautelares, dada la imposibilidad de ofrecer la prueba testimonial de abono que el Código Procesal exige, resulta absurdo y, tal vez, hasta contrario al artículo 31 de la Constitución Nacional.

A mi juicio, la brecha con el derecho sustancial que producen nuestras obsoletas normas procesales puede superarse recurriendo a doctrina y jurisprudencia elaboradas en derredor de otros supuestos.

Me explico: la doctrina ha indicado que la exigencia ritual de testigos de abono que reconozcan la firma del cautelado no es sacramental y puede sustituirse por otras pruebas, entre ellas, la certificación notarial, o el dictamen pericial[10]. Omar Díaz Solimine aclara que esta posibilidad se encuentra especialmente prevista en el artículo 523, inciso 2 del CPCC, respecto de los títulos ejecutivos instrumentados en documento privado suscripto por el obligado o cuya firma estuviese certificada por escribano con intervención del obligado y registrada en el protocolo, de modo que la aplicación analógica se impone[11].

---

[9] Artículo 7: "Presunción de autoría. Se presume, salvo prueba en contrario, que toda firma digital pertenece al titular del certificado digital que permite la verificación de dicha firma".

Artículo 8: "Presunción de integridad. Si el resultado de un procedimiento de verificación de una firma digital aplicado a un documento digital es verdadero, se presume, salvo prueba en contrario, que este documento digital no ha sido modificado desde el momento de su firma".

[10] Así, por ejemplo, Norberto José Novellino, *Embargo y desembargo y demás medidas cautelares*, cuarta edición, Abeledo Perrot, 1994, p. 61: "Coincidimos plenamente con los autores que sostienen la posibilidad de acreditar las firmas por otros medios de prueba en sustitución de la testimonial. Así se considera viable el informe bancario, las constataciones acumuladas en el juicio principal resultantes de la confesión de la contraria o de pericias"; Osvaldo A. Gozaini, *Tratado de Derecho Procesal Civil*, La Ley, 2009, t. I, p. 698.

[11] Comentarios al artículo 209 del CPCC, en Elena Highton y Beatriz Areán, *Código Procesal Civil y Comercial de la Nación*, Hammurabi, 2005, tomo 4, p. 283. En efecto, dicho artículo e inciso dicen: "Los títulos que traen aparejada ejecución son los siguientes: […] 2) El instrumento privado suscripto por el obligado, reconocido judicialmente o cuya firma estuviese certificada por escribano con intervención del obligado y registrada la certificación en el protocolo". Esta norma tampoco capta al instrumento electrónico privado con firma digital. Sin embargo, este es un equivalente funcional de aquél con una ventaja: un instrumento privado con firma certificada

Por su parte, la jurisprudencia —con cita de Lino Palacio— ha sostenido que "Resulta improcedente denegar la producción de cierta prueba pericial caligráfica para abonar la firma de un instrumento, toda vez que conforme lo previsto por el CPR 209-2, puede pedirse embargo preventivo en el caso de que la existencia del crédito esté demostrada con instrumento público o privado atribuido al deudor, abonada la firma por información sumaria de dos testigos. El precepto citado no excluye la posibilidad de que la autenticidad de la firma resulte de circunstancias ajenas a la información de abono, lo que ocurre, v. gr., si aquella se encuentra certificada por escribano o no ha sido desconocida por el defendido. Es obvio, por lo demás, que el pretensor puede prescindir de la mencionada información, que comporta un procedimiento instituido en su beneficio, y requerir, en cambio, la citación del presunto deudor en la forma prescripta para la preparación de la vía ejecutiva, siendo admisible, en caso de negativa, la práctica de prueba pericial (conf. Lino E. Palacio, *Derecho Procesal Civil*, Abeledo Perrot, 1992)"[12].

Según entiendo, nada se opone a que la doctrina y jurisprudencia reseñadas en el punto anterior se apliquen al caso de documentos electrónicos privados suscriptos mediante firma digital. En tales supuestos la información sumaria prevista por el artículo 209 incisos. 2 y 3 del CPCC parece devenir irrelevante: desde el punto de vista probatorio, la firma digital apli-

en "soporte papel" (o aun el testimonio de una escritura pública) es susceptible de alteraciones que pasen desapercibidas, en tanto que un instrumento privado electrónico firmado digitalmente ofrece seguridad adicional a través de la función *hash*, de modo que en casos así, la preparación de vía ejecutiva a través del procedimiento que regla el artículo 525, inciso 1 del CPCC también devendría irrelevante o resultaría suplantada con ventaja por la simple réplica del proceso de verificación de firma por parte del juez interviniente.

[12] Cámara Nacional en lo Comercial, Sala B, "Rimatori, Luis Alberto c/ Caja de Seguros de Vida S.A. s/ordinario", 14/2/03. Esta postura es, a mi juicio, la que indica el buen sentido. Novellino (*op. cit.*, nota 10, p. 138) recuerda la opinión de Augusto César Beluscio, quien critica que el CPCC "haya mantenido, en este artículo 209, inciso 2, la necesidad de abonar la firma del documento privado con la declaración de dos testigos y afirma: "Nadie ignora que en la generalidad de los casos este requisito obliga a recurrir a testigos falsos, pues no es ineludible que los instrumentos sean firmados delante de terceros". Y opina: "Creo que en estos casos bastaría con exigir el juramento acerca de la autenticidad del documento. Suficiente garantía es la responsabilidad por los daños y perjuicios y la comisión del delito previsto por el artículo 296 del Código Penal por quien obtiene un embargo preventivo sobre la base de un documento falso". Es claro, por otra parte, que la creación de documentos electrónicos bajo firma digital elimina inconvenientes como los señalados.

cada a un documento electrónico lo transforma en un equivalente funcional del instrumento público o, a lo menos, del instrumento privado con firmas certificadas y, en rigor de verdad, corre con la ventaja de la inalterabilidad que le otorga la función *hash* ínsita en el propio procedimiento de creación y firma. Bastaría, en todo caso, solicitar que el juez, por sí, replique el procedimiento de verificación de firma digital para constatar tanto la integridad del documento que se le presenta como la titularidad, validez y vigencia del certificado digital empleado por el cautelado para suscribirlo[13].

3. Vuelta al principio

De todo ello resulta —y, por supuesto, de no errar en mi razonamiento— que la firma digital o, si se quiere, el empleo en el tráfico jurídico de documentos electrónicos firmados digitalmente, facilita la *tutela judicial efectiva*, pues torna más expeditivo y transparente el procedimiento cautelar en base a instrumentos privados. Dicho de otro modo: provee un método rápido, sencillo, económico y seguro para acreditar, en base a un instrumento privado, la verosimilitud del derecho requerida como presupuesto de toda medida cautelar, de la que, a su vez y como dije al principio, depende la chance de obtener un ulterior pronunciamiento de mérito *útil*.

[13] Recuérdese que los artículos 8 y 9 de la Ley N.º 25.506 dicen:

Artículo 8: "Si el resultado de un procedimiento de verificación de una firma digital aplicado a un documento digital es verdadero, se presume, salvo prueba en contrario, que este documento digital no ha sido modificado desde el momento de su firma". El término *verdadero* refiere a la coincidencia (*match*) entre el *hash* del documento electrónico originalmente firmado mediante firma digital y la copia del documento presentada. Si ambos *hash* coinciden, el documento electrónico presentado es un ejemplar fiel del documento originalmente firmado, *tal como se lo firmó*. Si no coinciden, el documento presentado contiene alteraciones respecto de su original tal como se lo firmó.

Artículo 9: "Validez. 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. El procedimiento de verificación puede replicarse cuantas veces sea necesario, proveyendo un método sencillo para establecer la autoría e integridad de cierto documento electrónico, con las presunciones que de ello se derivan".

Los mecanismos alternativos de resolución de controversias como herramienta eficaz para facilitar la solución de conflictos en la contratación de software

por Ignacio de Castro, Leandro Toscano y Gonzalo Bleda

1. Introducción. La importancia del software y su contratación

El software tiene un presente y un futuro prometedor. En el presente, el software se ha integrado en el día a día de las empresas, formando en multitud de casos una parte esencial de sus procesos productivos. En el futuro, las características del software permiten pronosticar que las próximas tecnologías seguirán guardando una estrecha relación (quizás incluso de dependencia) con el software.

El software (comprendiendo tanto el código fuente como el código objeto) se entiende como una secuencia de instrucciones que se utiliza en un sistema informático para realizar una función o para obtener un resultado. Se trata de una definición fácilmente acomodable con distintas tecnologías como el *cloud computing*, la inteligencia artificial, la realidad virtual o los *smart contracts*. Todas estas tecnologías consisten y/o utilizan en mayor o menor medida un software (sea más o menos complejo o avanzado).

Es por esa relevancia que tiene el software que resultaba conveniente la publicación de una guía sobre aspectos legales del software, redactada con el objetivo de convertirse en una herramienta útil y práctica para las empresas, ya sean usuarios o proveedores de software. La guía para la redacción y negociación de contratos de software, la *Guía de Software*, de la Asociación Española de Derecho del Entretenimiento (DENAE), publicada en junio de 2018, es el resultado de un Grupo de Trabajo constituido a tal efecto por DENAE, y que contó con la participación del Centro de Arbitraje y Mediación de la Organización Mundial de la Propiedad Intelectual (Centro de la OMPI)[1].

[1] El Grupo de Trabajo fue coordinado por Miguel Ángel Mata y contó con la autoría de Gonzalo Bleda (quien actuó en nombre del Centro de la OMPI), Daniel Bulnes, Silvia Márquez, Miguel Ángel Mata, Gemma Minero, Joaquín Muñoz, Carlos Osuna y Helena Suárez. Se puede consul-

La *Guía de Software* se publicó con una finalidad informativa y divulgativa para que pueda servir a las partes de un contrato de software como una aproximación a los aspectos prácticos que generalmente resultan más relevantes en la redacción y en la negociación de un contrato que tiene por objeto un software o los servicios en torno a este.

El Grupo de Trabajo desarrolló la *Guía de Software* a través de un documento de trabajo colaborativo en torno a las cláusulas que se identificaron como las más relevantes en los contratos que tienen por objeto el software. Entre las distintas cláusulas que resultan especialmente relevantes en la negociación y redacción de un contrato de software, el Grupo de Trabajo identificó que las cláusulas sobre el objeto del contrato, los derechos y obligaciones de las partes, la propiedad intelectual, la terminación anticipada del contrato, la regulación de la responsabilidad, la protección de datos y la resolución de controversias tienen un impacto fundamental en este tipo de contratos.

Asimismo, dada la importancia y particularidad de los contratos de desarrollo, licencia y mantenimiento de software, cuando se identificaron diferencias reseñables, el Grupo de Trabajo analizó las peculiaridades de cada uno de estos tipos de contratos, desgranando las cláusulas más habituales en los contratos de licencia, desarrollo y mantenimiento de software. Además de las diferencias esenciales en cuanto al objeto y los derechos y las obligaciones que surgen de estos tres tipos de contratos, ha resultado necesario analizar otras cláusulas que guardan una estrecha relación con cada una de estas tipologías contractuales. Cláusulas como las que regulan los niveles de servicio (especialmente relevante en los contratos de mantenimiento), los derechos de uso y sus limitaciones (fundamental en el contrato de desarrollo y de licencia) o las cláusulas de auditoría (fundamentales para el control por los proveedores del software del uso que se va a dar del mismo) han sido objeto de análisis en la *Guía de Software*.

tar la *Guía de Software* en: http://bit.ly/2nwe1v0.

2. La identificación de potenciales aspectos conflictivos en la contratación en materia de software

La *Guía de Software* hace referencia a las distintas posiciones que las partes contratantes pueden adoptar a la hora de redactar y negociar un contrato. En este sentido, a lo largo de la *Guía de Software* se aborda una serie de problemas que los abogados de cada parte deben identificar durante las negociaciones con la contraparte y que deben prever durante la fase de redacción de los contratos. Además, en función de si actúan en nombre del proveedor o del cliente, los intereses que deberá representar el abogado serán distintos.

Sin pretender ser exhaustivos, identificamos a continuación algunos de los problemas que pueden surgir en la contratación de software:

1. ¿Cuáles son los derechos y el alcance de las obligaciones que corresponden a cada una de las partes?

2. ¿Cuál es el número de usuarios autorizados para utilizar el software en función del precio pagado y las condiciones contratadas?

3. ¿Pueden las empresas pertenecientes a un mismo grupo utilizar el software contratado por su empresa matriz? ¿Conllevaría alguna obligación adicional de pago?

4. ¿A quién corresponde la titularidad del desarrollo? ¿Se transfiere la titularidad del código fuente en un contrato de desarrollo? ¿Puede un desarrollador utilizar todo o parte del código fuente para desarrollar otro software para un tercero? ¿Es necesario que el cliente adquiera la titularidad de todos los derechos asumiendo el correspondiente coste o qué debe tenerse en cuenta a la hora de delimitar el alcance de que derechos debe adquirir el cliente?

5. Si se realiza un mantenimiento evolutivo o adaptativo del software que conlleve nuevos desarrollos, ¿a quién corresponde la titularidad de dichos nuevos desarrollos?

6. ¿Cómo se debe definir y delimitar el objeto del contrato? ¿Qué consecuencias puede acarrear una mala determinación de las funcionalidades del software?

7. ¿Qué sucede si un contrato de desarrollo de software se termina de manera anticipada antes de la entrega final del software y su apro-

bación por el cliente? ¿Qué derechos tiene el cliente? ¿Y el proveedor?

8. ¿Qué sucede cuando las expectativas de un cliente no se ven satisfechas por las funcionalidades de un software?

9. ¿Qué consecuencias se pueden derivar de la terminación anticipada de un software? Y si el software resulta fundamental para el desarrollo de un producto o la prestación de un servicio del c2liente que lo ha contratado, ¿cuál es entonces el impacto de la terminación? ¿Qué sucede si la sustitución del software por el cliente conlleva un coste elevado (ya sea en tiempo, en recursos humanos o económicos)?

Estos son sólo parte de los problemas que pueden surgir en la contratación de software. Todos estos y otros interrogantes deberían planteárselos los abogados a la hora de redactar los contratos correspondientes. Durante las fases de negociación y de redacción, los abogados tienen que anticipar los problemas, teniendo siempre presente cuál es el valor real del software para la empresa y qué impacto tiene en sus funciones esenciales si algo sale mal.

Sin perjuicio de la labor que deben de hacer los abogados durante la negociación y posterior redacción de los contratos de software, no hay que olvidar que los contratos se firman en un momento en el que los intereses de las partes están alineados, es decir, cuando la relación entre las partes es estable y saludable.

Es indudable que el abogado de cada parte tiene por objetivo conseguir el "acuerdo perfecto" para su representado, pero el hecho de que en un contrato confluyan posiciones contrapuestas con intereses diferentes, que además pueden evolucionar y cambiar, hace que la exhaustividad en el contrato resulte prácticamente inalcanzable, siendo imposible regular todos los problemas que podrían surgir en el futuro.

En este sentido, teniendo en cuenta que los intereses de cada parte pueden variar con el tiempo y las relaciones pueden deteriorarse, es fácil concluir que pueden surgir problemas e imprevistos que se deriven en un conflicto. Por ello resulta fundamental anticipar en los contratos potenciales problemas, conflictos y futuras controversias que se pueden dar en un activo como el software, que tiene un impacto directo en el negocio de las empresas.

3. El papel fundamental del abogado en la redacción y negociación de la cláusula de resolución de controversias

La redacción de las cláusulas de resolución de controversias tiene un valor fundamental. No hay que olvidar que cualquier problema que surja de un contrato se resolverá normalmente conforme a las cláusulas de resolución de controversias incluidas en dicho contrato. Si bien es cierto que las partes pueden acordar someter una controversia específica a un mecanismo distinto del que se regula en el contrato, la dificultad de alcanzar un acuerdo de sumisión cuando hay una controversia resulta muy elevada. Consultando las estadísticas respecto del origen de las controversias en los procedimientos que el Centro de la OMPI ha gestionado en materia de tecnologías de la información y de las comunicaciones (un 25% de las controversias gestionadas por el Centro de la OMPI son en materia de tecnologías de la información y de las comunicaciones) se desprende que la mayoría de los procedimientos gestionados tiene origen contractual.

Todo ello lleva a considerar el papel del abogado respecto de la resolución de controversias, que tiene una importancia doble:

· Por un lado, a la hora de anticipar los problemas, el abogado debe analizarlos e identificar las soluciones que resulten más eficientes (ya sea porque esa solución permite mantener la relación entre las partes, continuar con el desarrollo del proyecto y conseguir un buen resultado, ahorrar en tiempo o en coste, o buscar la solución del conflicto de manera confidencial minimizando posibles riesgos para la reputación). Las soluciones a los potenciales conflictos en materia de contratos de software dependen evidentemente de lo manifestado en la cláusula de resolución de controversias, de ahí la importancia de su redacción.

· Por otro lado, el abogado, dada su experiencia (y pericia técnica), debe poder identificar el nacimiento incipiente de una controversia. La identificación de una disputa en sus primeras fases puede permitir a las partes valorar si resulta conveniente la utilización de un mecanismo alternativo al fijado en la cláusula de resolución de controversias o incluso obtener información especializada para establecer que mecanismo es más eficiente. En estos casos, el artículo 4 del Reglamento de Mediación del

Centro de la OMPI prevé que una parte que desee proponer someter una controversia a mediación de la OMPI puede presentar una solicitud unilateral de mediación al Centro de la OMPI. Una vez recibida dicha solicitud, el Centro de la OMPI podrá ayudar a las partes a considerar la sumisión a mediación de la OMPI proporcionando información sobre el procedimiento de mediación de la OMPI. Si la otra parte estuviese interesada en participar en la mediación OMPI, deberá firmar y enviar la solicitud al Centro de la OMPI constituyendo dicho documento un acuerdo entre las partes de sometimiento a mediación.

En cualquier caso, resulta aconsejable que las partes lleven a cabo el ejercicio de identificación de problemas y soluciones en el momento de la redacción del contrato para determinar contractualmente el mecanismo de resolución de controversias más adecuado. Además, cualquiera de las partes (o ambas) pueden contactar con el Centro de la OMPI para obtener información sobre los distintos procedimientos y consejos sobre su adecuación a los contratos y a la naturaleza de los conflictos que puedan surgir de estos. Durante la fase de negociación y/o de redacción resulta más factible que las partes puedan alcanzar un acuerdo en torno a la cláusula de resolución de controversias que resulte más efectiva para las partes. Esta recomendación viene también amparada por las propias estadísticas del Centro de la OMPI, donde las controversias en materia tecnológica provienen en su gran mayoría del uso de una de las cláusulas de resolución de controversias que el Centro de la OMPI pone a disposición de las partes.[2]

Asimismo, ya sea en una fase de negociación y/o de redacción del contrato de software, ante el nacimiento de una controversia incipiente, o una vez surgida la disputa, el Centro de la OMPI puede ayudar a las partes a identificar el mecanismo específico que resulte más eficiente para la resolución de una controversia basándose en su experiencia en la gestión de procedimientos. De manera gratuita, a través de lo que se conoce como buenos oficios (o en inglés, g*ood offices*) el Centro de la OMPI puede aconsejar sobre el procedimiento más adecuado para que las partes intenten solucionar sus conflictos, ya sea mediante la negociación directa

[2] Más información respecto de las cláusulas: http://bit.ly/2ofFAsw.

entre las partes o valorando y ayudando a definir el mecanismo de resolución de controversias que mejor se adecue a las necesidades.[3]

En el Centro de la OMPI consideramos fundamental que las partes de un contrato de software puedan conocer y valorar qué mecanismos de solución de controversias tienen a su disposición para que una disputa se resuelva de la manera más eficiente posible.

El Centro de la OMPI como proveedor de servicios de resolución de controversias presta servicios para la gestión de procedimientos de mediación, arbitraje, arbitraje acelerado y procedimiento de decisión de experto (Mecanismos ADR del Centro de la OMPI).

4. Los Mecanismos ADR del Centro de la OMPI

4.1. La mediación como mecanismo de resolución de controversias

La mediación constituye un procedimiento de resolución de controversias de carácter consensual (las dos partes están de acuerdo en acudir a la mediación) que no culmina en una decisión impuesta de manera obligatoria a las partes. Las partes cuentan con la figura del mediador (un tercero experto en la materia y neutral respecto de las partes) para guiar la cooperación entre las partes, evaluar la controversia y facilitar que las partes alcancen acuerdo. Además, el carácter confidencial de la mediación permite a las partes discutir con franqueza posibles soluciones a una controversia, sin que las propuestas u ofertas de solución tengan impacto fuera del procedimiento de mediación.

En la mediación, el resultado viene determinado por la voluntad de las partes y la experiencia del mediador. La mediación permite a las partes la resolución de la controversia atendiendo principalmente a los intereses comerciales respectivos, teniendo en mente las repercusiones que una controversia mal gestionada puede tener en su relación. Así, la mediación puede resultar en un acuerdo entre las partes que tenga naturaleza contractual y que ponga fin al conflicto manteniendo con vida

[3] Más información respecto de la práctica de buenos oficios del Centro de la OMPI: http://bit.ly/2mBHBik.

la relación entre las partes. Conforme a las estadísticas del Centro de la OMPI en relación con los procedimientos de mediación, el 70% de las controversias que pasan por una mediación culminan en un acuerdo entre las partes.

Reproducimos a continuación la cláusula modelo del Centro de la OMPI para incluir en contratos en los que las partes acuerden someter sus controversias futuras a mediación:

> Toda controversia, diferencia o reclamación que surja del presente contrato y de toda enmienda al mismo o relativa al presente contrato, incluyendo en particular, su formación, validez, obligatoriedad, interpretación, ejecución, incumplimiento o terminación, así como las reclamaciones extracontractuales, serán sometidas a mediación de conformidad con el Reglamento de Mediación de la OMPI. La mediación tendrá lugar en [especificar el lugar]. El idioma que se utilizará en la mediación será [especificar el idioma].

4.2. Las ventajas de la inclusión de la mediación como mecanismo de resolución de controversias en cláusulas escalonadas

La mediación puede combinarse con otro tipo de procedimientos para la solución de controversias, ya sean mecanismos alternativos como el arbitraje o procedimientos tradicionales como la litigación ante tribunales. La utilización de cláusulas escalonadas en las que se combine la mediación con otro tipo de procedimientos plantea numerosas ventajas para las partes contratantes. En este sentido, las partes pueden acordar acudir a la mediación como primer mecanismo de solución de controversias seguido en ausencia de solución de arbitraje o de tribunales judiciales.

La mediación tiene un coste mucho menor que la litigación en tribunales o que el arbitraje, por lo que resulta en un mecanismo especialmente útil para un primer intento de solución del conflicto. A través de la mediación, las partes pueden alcanzar un acuerdo sobre la controversia o, incluso, formalizar una nueva base contractual que gobierne la relación entre las partes. Asimismo, la mediación permite identificar y establecer las posturas de las partes definiendo los intereses

comunes y contrapuestos, así como las estrategias con las que continuar en aras de la solución de la controversia.

En el caso de que el acuerdo no resulte posible en vía de mediación, en aquellos supuestos en los que se utilice una cláusula escalonada, siempre quedará la posibilidad de acudir al segundo mecanismo para la solución de controversias (ya sea el arbitraje o la litigación ante los tribunales judiciales). Este tipo de cláusulas contractuales combina la naturaleza consensual de la mediación (lo que permite mantener una buena relación entre las partes teniendo un menor coste tanto de tiempo como monetario) con la fuerza vinculante del arbitraje o de los tribunales judiciales en el supuesto de que las partes no hubieran sido capaces de resolver la controversia en la fase de mediación.

Reproducimos a continuación la cláusula modelo del Centro de la OMPI para la mediación seguida de arbitraje o arbitraje acelerado:

> Toda controversia, diferencia o reclamación que surja del presente contrato y de toda enmienda al mismo o relativa al presente contrato, incluyendo en particular, su formación, validez, obligatoriedad, interpretación, ejecución, incumplimiento o terminación, así como las reclamaciones extracontractuales, serán sometidas a mediación de conformidad con el Reglamento de Mediación de la OMPI. La mediación tendrá lugar en [especificar el lugar]. El idioma que se utilizará en la mediación será [especificar el idioma].
>
> Si la controversia, diferencia o reclamación no ha sido solucionada en la mediación, o en la medida en que no haya sido solucionada en el plazo de [60] [90] días contados desde el comienzo de la mediación, ésta será sometida a arbitraje, mediante la presentación de una solicitud de arbitraje por una de las partes, para su solución definitiva de conformidad con el Reglamento de Arbitraje [Acelerado] de la OMPI. No obstante, si antes de la expiración de ese plazo de [60] [90] días, una de las partes se abstiene de participar o deja de participar en la mediación, se someterá la controversia, la diferencia o la reclamación a arbitraje mediante la presentación de una solicitud de arbitraje por la otra parte para su solución definitiva de conformidad con el Reglamento de Arbitraje

> [Acelerado] de la OMPI. [El Tribunal Arbitral estará compuesto por [un árbitro único] [tres árbitros].][4] El arbitraje tendrá lugar en [especificar el lugar]. El idioma que se utilizará en el procedimiento arbitral será [especificar el idioma]. La controversia, diferencia o reclamación sometida a arbitraje se resolverá de conformidad con el derecho de [especificar la jurisdicción].

4.3. El arbitraje y el arbitraje acelerado como mecanismos de resolución de controversias

En el arbitraje las dos partes están de acuerdo en acudir a este mecanismo para la solución de las controversias culminando el arbitraje en un laudo de carácter vinculante para las partes (sin perjuicio de que también existe la posibilidad de que las partes alcancen un acuerdo e incluso que se solicite al árbitro la emisión de un laudo aceptado en el que se incorpore el acuerdo de las partes).

Uno de los principales beneficios que plantea el arbitraje es que el laudo es vinculante para las partes y ejecutable internacionalmente como consecuencia de la Convención sobre el Reconocimiento y la Ejecución de las Sentencias Arbitrales Extranjeras, Nueva York, 1958 (Convenio de Nueva York), del cual, a fecha de 2018, 159 estados son parte. El laudo es obligatorio para las partes, definitivo (la posibilidad de recurso es limitada), y cuenta con la misma fuerza ejecutiva que una sentencia judicial.

En contraposición con la litigación ante los tribunales, el arbitraje dota a las partes de mayor flexibilidad lo que permite definir y adaptar el procedimiento a las necesidades de la controversia. Las partes pueden elegir árbitros que sean expertos no sólo en un área específica del derecho sino que tengan experiencia también en contratos tecnológicos o en la industria del software.

En el arbitraje, el derecho aplicable al proceso del arbitraje es la ley que rige el marco procedimental, por lo general la ley arbitral del lugar

[4] El Reglamento de Arbitraje Acelerado de la OMPI provee que el tribunal arbitral estará compuesto por un solo árbitro.

elegido para el arbitraje (es decir, determinando el lugar del arbitraje las partes eligen el derecho arbitral)[5]. No es necesario que el derecho aplicable al proceso del arbitraje sea el mismo que el derecho aplicable al fondo. Además, con independencia del lugar del arbitraje, conforme al Reglamento de Arbitraje de la OMPI, el tribunal arbitral podrá consultar previamente con las partes la celebración de las audiencias en el lugar que considere apropiado. Es decir, la determinación del lugar del arbitraje en la cláusula conlleva que el laudo del tribunal arbitral se considere dictado en dicho lugar (ello con independencia de que las audiencias puedan llevarse a cabo en otro lugar).

Asimismo, si la celeridad en la resolución de la controversia resulta un factor esencial las partes, puede optar por acudir al arbitraje acelerado de la OMPI, donde se condensan las principales etapas del arbitraje, lo que permite concluir el proceso en un plazo menor de tiempo.

Reproducimos a continuación la cláusula modelo del Centro de la OMPI para incluir en contratos en los que las partes acuerden someter sus controversias futuras a arbitraje o arbitraje acelerado:

> Toda controversia, diferencia o reclamación que surja del presente contrato y de toda enmienda al mismo o relativa al presente contrato, incluyendo en particular, su formación, validez, obligatoriedad, interpretación, ejecución, incumplimiento o terminación, así como las reclamaciones extracontractuales, serán sometidas a arbitraje para su solución definitiva de conformidad con el Reglamento de Arbitraje [Acelerado] de la OMPI. El tribunal arbitral estará compuesto por [un árbitro único] [tres árbitros].[6] El arbitraje tendrá lugar en [especificar el lugar]. El idioma que se utilizará en el procedimiento arbitral será [especificar el idioma]. La controversia, diferencia o reclamación se resolverá de conformidad con el derecho de [especificar la jurisdicción].

[5] Cabe destacar que desde julio de 2018 la Argentina cuenta con una Ley de Arbitraje Comercial Internacional N.º 27.449, en consonancia con los principios internacionales de esta práctica.

[6] El Reglamento de Arbitraje Acelerado de la OMPI provee que el tribunal arbitral estará compuesto por un solo árbitro.

4.4. Estudio de caso de uso de los procedimientos ADR del Centro de la OMPI en materia de controversias de software por parte de un grupo empresarial

A continuación analizamos los datos respecto de la utilización los procedimientos ADR del Centro de la OMPI por parte de sociedades de un mismo tipo de empresas que operan en la industria del software.

Antecedentes:

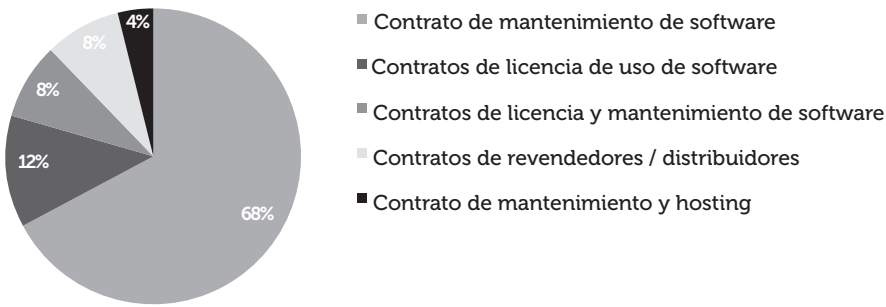
· El grupo de empresas ha iniciado **25 mediaciones** ante el Centro de la OMPI relativas a controversias en materia de software.

· El grupo empresarial incorpora en sus **términos y condiciones** una cláusula escalonada de **mediación seguida de arbitraje acelerado ante el Centro de la OMPI**. Ello implica que el primer mecanismo que las partes utilizaron para resolver su controversia es la mediación solo acudiendo al arbitraje acelerado en caso de ausencia de solución en la mediación.

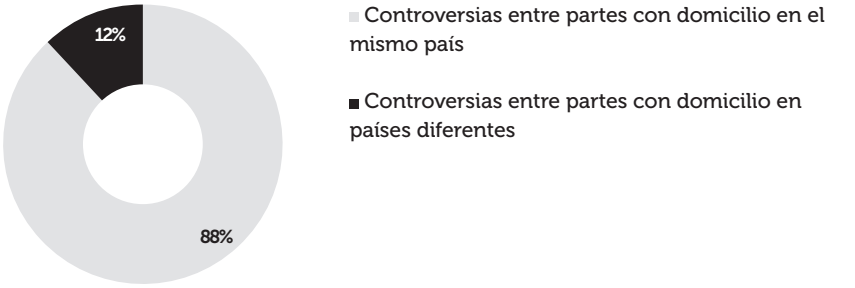
· La matriz del grupo empresarial se encuentra ubicada en Estados Unidos de América, si bien desarrollan su actividad empresarial de manera internacional.

· De **25** solicitudes de **mediación** presentadas ante el Centro de Arbitraje y Mediación de la OMPI, solo 3 casos llegaron a la fase de arbitraje acelerado.

Tipología de los contratos



Ámbito territorial de las controversias



· El **57%** de los casos se resolvió con un **acuerdo** de las partes tras presentarse la solicitud de mediación. Sin perjuicio de lo cual, parece que pudo haber casos en los que las partes **alcanzaron un acuerdo fuera del procedimiento de mediación** en tanto que no se inició el procedimiento de arbitraje.

· Un **38%** de los acuerdos de las partes se concluyó luego de iniciada la mediación y **antes del nombramiento del mediador**.

· Solo en el **13%** de los casos terminados sin acuerdo de partes se inició el **arbitraje acelerado**.

· **3 meses** de duración media.

· Tiene un coste medio de **1.500** dólares, incluyendo tasas administrativas y honorarios del mediador (en los casos en los que se nombró al mediador).

5. Conclusiones

La contratación en materia de software puede contribuir en la mejora de la productividad (y causar un impacto importante en los procesos productivos y de prestación de servicios) de las empresas. Tanto los clientes como los proveedores de software deben ser conscientes de la importancia que tiene la adecuada redacción y negociación de este tipo de contratos, así como de las necesidades de la relación comercial que surge de estos.

En dichos procesos de redacción y negociación de los contratos, resulta fundamental el papel del abogado para identificar aquellos aspectos conflictivos que pudieran dar lugar a una controversia en el futuro y afec-

tar a la relación entre las partes. El abogado debe tratar de anticipar posibles conflictos para considerar el mecanismo de resolución de controversias que resulte más eficiente y que así quede reflejado en el contrato.

Como demuestra el estudio del caso mencionado anteriormente, la elección de una cláusula de resolución de controversias escalonada plantea numerosas ventajas para las partes de un contrato de software. En aquellos supuestos en los que las partes opten por la litigación en tribunales judiciales, la inclusión de una fase previa de mediación a través de una cláusula escalonada permite a las partes beneficiarse de la mediación (que tiene generalmente un menor coste) sin que se vea afectada la relación comercial entre las partes por el desgaste y/o agresividad de la litigación.

Asimismo, para maximizar los beneficios que ofrecen los mecanismos ADR del Centro de la OMPI, las partes pueden también combinar los diferentes procedimientos comenzando, por ejemplo, con una fase de mediación, a seguir en ausencia de solución por una fase de arbitraje. La combinación de la mediación con el arbitraje permite que si las partes no alcanzan un acuerdo en la fase de mediación (donde en estadísticas del Centro se alcanza un acuerdo en el 70% de los casos) puedan intentar alcanzarlo dentro del arbitraje (en la experiencia del Centro de la OMPI, aproximadamente el 40% de los procedimientos de arbitraje ha terminado con un acuerdo amistoso entre las partes) o si el acuerdo no es posible, el conflicto se resuelva de manera final mediante un laudo arbitral ejecutable internacionalmente.

Alrededor del 40% de los procedimientos presentados ante el Centro de la OMPI incluyó una cláusula escalonada que preveía la mediación de la OMPI seguida, en ausencia de una solución, por arbitraje acelerado o arbitraje de la OMPI.

¿Contratos inteligentes o software obediente?

por Andrés Chomczyk

Resumen: Este trabajo tiene por finalidad estudiar el tratamiento normativo que les cabe a los llamados contratos inteligentes, o *smart contracts*. Si bien la idea de este tipo de contratos tiene más de veinte años, recién con la aparición de la tecnología *blockchain* se han comenzado a proponer soluciones concretas que puedan hacer uso de estos instrumentos para mejorar la contratación entre personas en el mundo digital.

A lo largo del artículo realizaremos un estudio de los conceptos técnicos que componen a esta nueva herramienta que propone automatizar el cumplimiento y la ejecución de los contratos, así como de sus supuestos beneficios y también de sus problemas. No solo analizaremos la cuestión desde lo teórico, sino que veremos un caso práctico y los problemas que se han presentado en este. Tras ello, estudiaremos algunas de las incipientes conclusiones del Derecho comparado para luego volcarnos a estudiar cómo encuadrar jurídicamente los contratos inteligentes dentro del marco normativo argentino. En particular, analizaremos si, dadas ciertas condiciones preexistentes, los contratos instrumentados mediante software pueden dar cumplimiento al requisito de forma establecido por el Código Civil y Comercial de la Nación. Finalmente, se hará un pequeño comentario sobre los límites impuestos por el orden jurídico al uso de estos instrumentos.

Abstract: The purpose of this paper is to study the normative treatment that fits the so-called smart contracts. Although the idea of this type of contract is more than twenty years old, only with the emergence of blockchain technology, concrete solutions have been proposed that can make use of these instruments to improve contracting among people in the digital world.

Throughout the article we will carry out a study of the technical concepts that make up this new tool that proposes to automate the fulfillment and execution of contracts as well as their supposed benefits and also their problems. We will not only analyze the question from the theoretical point of view but we will also see a practical case and the problems that have been presented in it.

After that, we will study some of the incipient conclusions of comparative law and then turn to study how to frame legally intelligent contracts within the Argentine regulatory framework. In particular, we will analyze whether, given certain pre-existing conditions, contracts implemented through software can comply with the requirement established in the Argentine Civil and Commercial Code. Finally, some comments will be made on the limits imposed by the legal order on the use of these instruments.

Palabras clave: contratos inteligentes, contratos electrónicos, blockchain, firma digital, firma electrónica.

Keywords: smart contracts, electronic contracts, blockchain, digital signature, electronic signature.

1. Introducción

La idea de contratos inteligentes suele ser atribuida a Nick Szabo, uno de los criptógrafos más importantes de la actualidad, quien introdujo el concepto en el marco de una economía cada vez más digitalizada[1]. En aquella oportunidad, describió a los contratos inteligentes como un conjunto de cláusulas contractuales insertadas directivamente en el hardware o el software y que tienen por finalidad regular la relación jurídica subyacente automatizando la ejecución del acuerdo y dejando de lado toda intervención humana.

Frente a esta realidad, la pregunta que nos hacemos como juristas es si los contratos inteligentes, o s*mart contracts*, son efectivamente contratos. En otras palabras, debemos preguntarnos si estamos frente a instrumentos legales que contienen una relación jurídica con capacidad para decidir por sí mismos, así como también ser autosuficientes para la ejecución y el cumplimiento de aquella, o bien, lo que tenemos delante de nosotros es software obediente[2] que sigue las instrucciones impartidas

[1] Cfr. Szabo, Nick: "The Idea of Smart Contracts" [http://bit.ly/2LKVG7P].

[2] La idea de considerar a los contratos inteligentes como meras herramientas informáticas para facilitar ciertos aspectos de las relaciones jurídicas contractuales pactadas entre las partes

por las partes de un verdadero contrato jurídico instrumentado en otro soporte diferente del software o hardware donde estos supuestos términos contractuales están insertados.

En consecuencia, el presente trabajo tiene por finalidad indagar sobre la posibilidad de considerar a los contratos inteligentes, o *smart contracts*, como contratos, según el nuevo Código Civil y Comercial de la Nación (CCyCN). Este trabajo consta de tres secciones: *(i)* en una primera etapa introduciremos el concepto de contrato inteligente y los beneficios que llaman a su adopción en la creciente economía digital, así como algunas de las críticas que han recibido; *(ii)* en segundo lugar, señalaremos algunos de los desafíos jurídicos que ya han comenzado a aparecer a nivel internacional con relación a estos y las primeras conclusiones que el Derecho comparado ha tenido frente a este fenómeno; y *(iii)* por último, trabajaremos sobre si es posible considerarlos como contratos a la luz del nuevo CCyCN.

2. Concepto de contrato inteligente. Beneficios y soluciones. Críticas e identificación de problemas

Tal como definimos en la introducción, los contratos inteligentes buscan regular las relaciones jurídicas que se producen como consecuencia de la interacción del software o hardware con una determinada realidad. Volviendo a los conceptos de Szabo,[3] la propuesta por la creación de contratos inteligentes está relacionada con los cambios en la forma de crear instrumentos legales. En la actualidad, la redacción de contratos se encuentra basada en medios y formas estáticas, cuya interpretación siempre recae sobre los seres humanos, sin perjuicio de usar herramientas tecnológicas para facilitar estas tareas. Ahora bien, en la actualidad contamos con elementos técnicos que nos permiten usar medios y formas dinámicas que pueden ser interpretados por la misma tecnología. Szabo nos propone asimilar y equiparar los términos técnicos a los términos legales y hacer que el código, es decir el software, sea la ley para las partes de aquella relación jurídica.

en el mundo físico ha sido propuesta por Cristina Carrascosa, jurista española especialista en *blockchain*. Ver: http://bit.ly/2uZ1H75.

[3] Cfr. Szabo, Nick, *Formalizing and Securing Relationships on Public Networks* [http://bit.ly/2LNmTqn].

Aunque normas recientes, como el nuevo CCyCN, contienen provisiones para los casos de contratación electrónica así como también sobre el uso de soportes digitales para la instrumentación de acuerdos y la expresión de la voluntad, estas regulaciones siguen partiendo del esquema anterior de redacción, cumplimiento y ejecución basado en la interacción humana y el uso del "lenguaje humano", como factor clave para regir estos acuerdos. Este tipo de contratos son económicamente ineficientes; Szabo[4] sostiene que los contratos realizados en un soporte digital pero con lenguaje humano tienen aparejados, en su esencia, los mismos costos transaccionales que sus equivalentes en papel.

El lenguaje humano está sujeto a interpretación y cada operador jurídico puede tener una interpretación diferente; el lenguaje computacional es fundamentalmente binario, lo cual disminuye en forma considerable las posibilidades de interpretación y, consecuentemente, de errar en aquella.

Szabo[5] sostiene que los contratos inteligentes reducen los costos de transacción, es decir, todos los controles, chequeos y procedimientos que deben ser realizados por terceros de confianza para redactar el contrato, vigilar su cumplimiento y efectivizar su ejecución en caso de incumplimiento. En este nuevo paradigma digital, donde la tecnología permite la introducción de instrucciones de comportamiento en el mismo hardware o software, hace posible que estos controles, chequeos y procedimiento sean llevados a cabo por el mismo componente tecnológico, bajo la forma de un protocolo que automatice estas actividades, eliminando así la interacción humana y las deficiencias asociadas a esta.

Siguiendo con este análisis, podemos decir que los protocolos son más eficientes que los controles, chequeos y procedimientos realizados por los humanos en tres campos: forma, confidencialidad y ejecución. Primero, la forma que tienen los seres humanos de controlar y efectivizar el cumplimiento de los contratos suele ser estandarizada para permitir que cualquier nuevo revisor pueda fiscalizar sin problema los contratos que tiene a su cargo. Por otro lado, los protocolos suelen implicar formas ajustables a cada entorno en el cual son desplegados, pudiendo elimi-

[4] Cfr. Ibídem.
[5] Cfr. Ibídem.

nar elementos innecesarios que hacen más onerosa la tarea en cuestión. Segundo, dado que los controles implican la intervención de otras personas distintas de las partes del contrato, estos ponen poco énfasis en la confidencialidad, y de allí que resulte necesario recurrir a otros controles, como por ejemplo convenios de confidencialidad, para limitar la publicidad de los términos del acuerdo. Por su parte, en un protocolo basado en la criptografía, permite la protección de la información confidencial sobre una determinada relación jurídica desde su génesis. Finalmente, para la ejecución de los controles es necesario un equipo específico de personas previamente designadas por las partes, mientras que en un protocolo es un software que integra la relación jurídica el encargado de vigilar el cumplimiento del acuerdo.

A criterio de Szabo,[6] el contrato inteligente es eficiente si existe desde el nacimiento de la relación contractual; tomar una relación jurídica contractual tradicional y transformarla en "inteligente" es poco eficiente, económicamente hablando, ya que implicaría una duplicación de los esfuerzos y de los costos.

La explosión tecnológica ha introducido una serie de variables, como el mayor grado de activos que nacen digitales, que resultan propicias para ser aprovechadas para la proliferación de los contratos inteligentes. El problema con los activos digitales que demoró la utilización de estos instrumentos fue la facilidad para realizar copias de estos activos y la imposibilidad de controlar su escasez. Esto se intentado resolver mediante la aplicación de tecnologías de gestión de derechos, como los DRM, pero no han tenido éxito debido a la facilidad con la que estas medidas tecnológicas han sido violadas. Recién con la aparición de la tecnología *blockchain* y la solución al problema del doble gasto[7] se ha comenzado a considerar que existen elementos técnicos para hacer realidad estas ideas. El uso de tecnología *blockchain* no es menor porque permite que entidades que no confían entre sí lo hagan sin recurrir a un tercero, cuya existencia implica un costo para las partes. Si sobre esa red descentralizada donde están los activos digitales es posible crear acuerdos contractuales

[6] Cfr. Ibídem.

[7] Al respecto, recomendamos la lectura del siguiente artículo: Chohan, Usman, "The Double Spending Problem and Cryptocurrencies" [http://bit.ly/2v1D3Tm].

digitales para regir las relaciones jurídicas entre las partes que permitan la ejecución y fiscalización automática de los mismos, podemos decir que ese acuerdo será un contrato inteligente.

Siguiendo a Szabo,[8] en la redacción de contratos hay tres cuestiones sobre las cuales poner el foco para una buena redacción de estos: la observación del cumplimiento por las partes, la posibilidad que un tercero de confianza pueda verificar el cumplimiento del contrato y la privacidad del contenido del contrato. En estas tres áreas pueden ser de utilidad los contratos inteligentes y, en particular, el uso de redes distribuidas basadas en el uso de seudónimos, independientes de cualquier tercero, como por ejemplo la tecnología *blockchain*. Uno de los temas principales sobre los que se habla a la hora de analizar la eficiencia de los *smart contracts* es su autosuficiencia para garantizar el cumplimiento del contrato.

Los contratos tradicionales, en última instancia, tienen su ejecución garantizada mediante el sistema jurídico que conocemos. Siempre es posible el reclamo judicial de la prestación debida. Ahora bien, esta posibilidad no es gratuita ni, en la gran mayoría de los casos, ágil. Es por ello que las partes, en los contratos tradicionales, establecen mecanismos para evitar recurrir a la justicia impartida por el Estado. Es aquí donde los contratos inteligentes pueden brillar. Los contratos inteligentes, al ser código insertado en el mismo objeto del contrato, apuntan no solo a regular el cumplimiento del contrato sino también a facilitar y automatizar la ejecución de este en caso de incumplimiento. Los *smart contracts* pueden ser vistos también como un mecanismo sofisticado de resolución de controversias de forma privada.

Es posible adoptar medidas proactivas, antes del incumplimiento, o reactivas, postincumplimiento, para garantizar el cumplimiento de un contrato. Tal como señala toda la doctrina en la materia, resulta más eficiente prever medidas para garantizar el cumplimiento que medidas para corregir un incumplimiento. Aquí es donde entra en juego una separación de contratos inteligentes propuesta por Max Raskin,[9] quien clasifica los *smart contracts* en fuertes y débiles. Los primeros son aquellos cuyos

[8] Cfr. Szabo, ídem.

[9] Raskin, Max: "The Law and Legality of Smart Contracts", *Georgetown Law Technology Review*, 2017, p. 305.

costos para litigar un problema en torno a los mismos es alto o prohibitivo, mientras que los segundos admiten la posibilidad de litigarlos puesto que el costo del recurso judicial es inferior al costo de admitir la ocurrencia de la consecuencia programada.

Tal como sigue detallando Raskin en su artículo, la adopción de medidas proactivas para asegurar el cumplimiento de un contrato es simplemente trasladar la interpretación y ejecución del contrato de una persona con facultades para hacerlo —un juez, un árbitro, etcétera— a una computadora. En un ambiente como el propuesto por Szabo, donde los bienes, los acuerdos y las relaciones jurídicas tienen lugar en redes digitales públicas, como puede ser una *blockchain*, es lógica la implementación de contratos inteligentes para evitar ese paso ineficiente entre el mundo físico y el mundo digital. Lo que nos preguntamos a continuación es cómo insertamos esta nueva realidad en nuestro sistema jurídico y si esto es posible.

Ahora bien, también existe parte de los expertos que no consideran a estos contratos como tales y que, incluso, ponen en duda su inteligencia y pretendida autosuficiencia de estos. En este sentido, podemos mencionar a Jimmy Song, informático especialista en criptomonedas y *blockchain*, quien intenta disipar las dudas y los mitos sobre los contratos inteligentes[10]. Según su criterio, estos contratos no son inteligentes porque solo pueden comportarse siguiendo las instrucciones previstas por las partes a la hora de redactarlos; cualquier situación que ocurra y que no haya sido prevista por las partes, deja al *smart contract* totalmente inutilizado. Un verdadero contrato inteligente debería comportarse como un juez, es decir, como una entidad que pueda resolver un conflicto no previsto por las partes originalmente y que dicha solución sea apropiada y ajustada a Derecho.

Este problema encuentra su razón de ser en la complejidad que tienen los contratos inteligentes para ser redactados de forma adecuada. A medida que la relación jurídica a ser regulada se torna más compleja, el software también debe volverse más complejo; para ilustrar esto, más adelante analizaremos el caso de un contrato inteligente que falló en la práctica. Si se pre-

[10] Cfr. Song, Jimmy: "The Truth about Smart Contracts" [http://bit.ly/2uYM4gb].

tende que el contrato inteligente sea autosuficiente, necesita herramientas para hacerlo. Pretender codificar en software toda la realidad es tan absurdo como pretender que un contrato contenga todos los supuestos posibles que hacen a una relación jurídica. Inevitablemente será necesario recurrir a elementos normativos generales, como una norma o un principio, para resolver un problema o situación no previsto en el acuerdo.

No solo resulta complejo y dificultoso representar una relación jurídica mediante código, sino que también existe el problema de la efectiva autosuficiencia del contrato inteligente. En la medida en que toda la información sobre el contrato se encuentre digitalizada en una base de datos en la que las partes del acuerdo puedan confiar, y esa base de datos automatizada esté en funcionamiento, es posible la existencia de un verdadero contrato inteligente. Caso contrario, estaríamos teniendo que recurrir a intervenciones humanas bajo la figura de los denominados "oráculos", quienes pueden aportar información sobre el mundo "físico" y, nuevamente, introduciendo la interpretación humana y los costos asociados a la misma, junto con la eliminación de la autosuficiencia de los elementos digitales. Esto implica que no solo introducimos la complejidad de la redacción de un contrato inteligente, sino que seguimos dependiendo de la interpretación humana para resolver un determinado problema.

3. Primeros análisis realizados en el Derecho comparado

Ante los nuevos desafíos profesionales que los abogados debemos enfrentar, solemos observar la posición que adoptaron otras jurisdicciones frente a nuevos fenómenos cuando se trata de cuestiones donde la ley todavía no ha llegado para ver si los esfuerzos que otros colegas han realizado son útiles para nuestro análisis.

En este sentido, podemos mencionar, por ejemplo, a Rosine Kadamani, quien sostuvo que un contrato inteligente no es un concepto jurídico sino que es un concepto creado en el mundo de la tecnología y se asocia con un sistema inteligente; la idea es que se programe una red de manera que, si la red percibe que un evento X ocurrió, la red va actuar de

una manera Y, sin interferencia humana[11]. Es decir, para la jurista brasileña los contratos inteligentes no son contratos en sí mismos pero pueden ser la forma de contrato en ciertos casos o un instrumento usado en el marco de una relación jurídica. Lo importante para esta autora radica en identificar los campos de cada cuestión, es decir, identificar la existencia de los requisitos que cada ordenamiento jurídico establezca para la existencia de un contrato.

Por su parte, Raskin[12] ha considerado que mientras se reúnan los elementos que integran un contrato tradicional en el contrato inteligente, ello será suficiente para darle validez legal al conjunto del software usado como instrumento para organizar esa relación jurídica. A criterio de este autor, el problema de los *smart contracts* no está en la etapa de formación del contrato ni en su ejecución, sino en cómo integrar su revisión judicial con la autonomía y autosuficiencia que posee este instrumento, en particular en lo que hace a la interpretación de este. Para Raskin, la legislación puede ser el único camino apto para encausar cualquier problema que pueda tener un contrato inteligente. A modo de ejemplo, Raskin sostiene que los *smart contracts* deberían estar conectados mediante una API a una base de datos pública de leyes y estar chequeando constantemente si los términos del acuerdo codificados en el software son compatibles con la ley. Mientras las partes se encuentren en el campo de la autonomía de la voluntad y de los medios alternativos de resolución de controversias, los contratos inteligentes podrían ser usados libremente.

Dos juristas ingleses, Andy Robinson y Tom Hingley, han considerado que los contratos inteligentes son efectivamente otra forma que pueden adoptar los contratos que, insertados en nuevos paradigmas tecnológicos, como *blockchain*, pueden dar lugar a interacciones y soluciones contractuales mucho más efectivas que sus contrapartes analógicas[13]. Es

[11] Cfr. Kadamani, Rosine: exposición realizada durante laBITconf 2016 en el panel "Legal Challenges" realizada en la Ciudad de Buenos Aires, 4 y 5 de noviembre de 2016. Video de la exposición disponible en: https://youtu.be/euFJ1QiGmzg.

[12] Cfr. Raskin, ídem, pp. 321 y ss.

[13] Cfr. Robinson, Andy & Tom Hingley: "Smart Contracts: the Next Frontier?", *Business Law*, blog de la Facultad de Derecho de la Universidad de Oxford, 23 de mayo de 2016 [http://bit.ly/2LHXe2i]. También cfr. Robinson, Andy & Tom Hingley: "A Smart New

interesante señalar que, según estos abogados, los *smart contracts* pueden ser usados para cualquier tipo de contrato y que, en principio, un contrato inteligente es un contrato, sin importar la materia o su contenido.

Los autores ponen el foco del análisis sobre dos cuestiones, íntimamente vinculadas: cómo se redacta el contrato inteligente y quién es responsable por su redacción. Sobre la primera cuestión, señalan que los abogados, quienes tradicionalmente escribían los contratos, deberán ajustar sus habilidades de redacción para incorporar el código como nuevo lenguaje; sin perjuicio de ello, también señalan la necesaria intervención de los especialistas para la correcta "traducción" de las cláusulas legales en cláusulas tecnológicas. Por otro lado, también ponen el foco en la responsabilidad derivada de la propia redacción del contrato inteligente. En este sentido, los autores sostienen que, ante la ausencia de normativa específica, son de aplicación los principios generales de la responsabilidad, incluyendo resolver cuestiones como la aplicación de criterios de imputación subjetivos u objetivos, determinar la existencia o no de conductas antijurídicas, o bien identificar qué conductas guardan causalidad con el daño sufrido.

Por último, repasaremos un comentario que han realizado algunos juristas de ENATIC[14]. Dicho artículo realiza un análisis muy parecido al que haremos cuando veamos este fenómeno desde la óptica del Derecho argentino. Para estos abogados, los elementos contra los cuales se deben analizar los contratos inteligentes son el Código Civil y la Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico. Si el *smart contract* cumple con los requisitos establecidos para la existencia de un contrato legal, estaremos frente a un contrato vinculante para las partes. El Código Civil regula las generalidades del instrumento, mientras que la segunda norma trata sobre las particularidades del soporte electrónico usado para materializar el contrato inteligente.

En general podemos observar que casi toda la doctrina disponible en la materia coincide en que los *smart contracts* son una forma que pueden adoptar los contratos para facilitar algunos de sus aspectos. Es decir, los

World: Blockchain and Smart Contracts" [http://bit.ly/2uZLIG1].

[14] Cfr. Blanco Pérez, Marelisa Andrea, López Román, Eduardo – Montalván Calderón, Erika Suárez Otero, Emilio – Farran Castellá, Pere – Espinoza Valencia, Félix Fabián,: "Contratos inteligentes: los 'smart contract'" [http://bit.ly/2v18HQZ].

contratos inteligentes son parte de nuestro ordenamiento jurídico y deberían ser analizados dentro de este marco.

4. El caso "The DAO"

Siguiendo con las críticas que habíamos señalado anteriormente a la idea de los contratos inteligentes, pasaremos a analizar un caso en el que varios de los problemas de los *smart contracts* se hicieron realidad. El caso "The DAO" ha sido el primer ejemplo de un contrato inteligente que ha fallado[15]. The DAO era una llamada organización autónoma descentralizada, un tipo de contrato inteligente, que buscaba actuar como plataforma de financiamiento colectivo de proyectos corriendo bajo su código, imitando el comportamiento de un fondo común de inversión y siendo el código el instrumento constitutivo y reglamento de gestión del mismo. Para ser parte de este vehículo de inversión, era necesario entregar fondos, en forma de la criptomoneda *ether* (la criptomoneda de la red Ethereum), y a cambio se recibían "títulos" de propiedad, similares a una cuota parte de un fondo común de inversión, en forma *tokens* de The DAO[16].

La idea jurídica central de The DAO era la separación del sistema jurídico vigente y la autosuficiencia del código respecto del Derecho "tradicional" para resolver toda situación que pudiera derivarse del funcionamiento de este contrato inteligente; esto implicaba que el Derecho y la jurisdicción aplicable al contrato entre los tenedores de *tokens* de The DAO era el mismo código donde The DAO corría. No había situación que pudiera darse fuera de lo contenido en el código. El problema de The DAO fue que, aun dentro del código, podían tener lugar escenarios no previstos por las partes intervinientes en la confección de los términos que integrarían el acuerdo.

En junio de 2016, un tenedor de *tokens* de The DAO dispuso la utilización de una función que estaba prevista en el código para retirar su participación en el contrato inteligente y convertir sus *tokens* de The DAO en *ether*, es decir, hacer el proceso inverso de ingreso para salir del

[15] Una breve y clara explicación en inglés de The DAO puede ser consultada en: http://bit.ly/2v0euGp.

[16] Para mayor información sobre el concepto de *token*, ver referencias incluidas en la nota al pie 21.

vehículo de inversión. Ahora, el código presentaba ciertas deficiencias en su redacción que permitían volver a ejecutar esta función mientras la misma función ejecutada previamente estaba corriendo. Esto derivó en un ciclo interminable donde el atacante estaba constantemente retirando sus fondos originales. El incidente fue tan grave que la comunidad de Ethereum planteó un debate sobre la efectiva inmutabilidad de las cadenas de bloques y sobre qué correspondía hacer: si "honrar" la ley del contrato —es decir, el código—, permitiendo el robo antes mencionado, o revertir la situación "borrando" lo pactado por las partes a la hora de adherir a The DAO y empleando elementos jurídicos no previstos en el código, principalmente el principio de buena fe en la ejecución de los contratos, para resolver el problema.

Este caso dio lugar a muchas de las primeras reflexiones sobre casi todos los aspectos posibles de los *smart contracts*: desde su naturaleza jurídica hasta quién es responsable por los daños y perjuicios derivados del contrato inteligente pasando por si una organización autónoma descentralizada es efectivamente un sujeto de derecho o no. Claramente muchos de temas, que son importantes y merecedores de análisis por separado, exceden el marco de este trabajo.

En uno de los análisis más completos sobre el caso se reflexiona sobre la naturaleza jurídica del s*mart contract* que formaba The DAO[17]. En dicho artículo, el autor intenta determinar si estamos frente a un contrato, en sentido legal, o bien si estamos frente a otra situación que ha sido denominada contrato por una convención. Haciendo una lectura de los distintos elementos que integraban a The DAO, desde los términos y condiciones de la pagina web, el código mismo, las licencias de software a las cuales se remitía y otros documentos vinculados, el autor no puede llegar a una conclusión y sostiene que es necesaria una determinación judicial de la cuestión. Los documentos son, a su criterio, al menos contradictorios. Lo único sobre lo cual está seguro es que, en caso de considerar a The DAO como un contrato, este tiene que ser necesariamente un contrato por adhesión. Debido a la cantidad de "documentos" legales, era

[17] Cfr. Hinkes, Drew: "A Legal Analysis of the DAO Exploit and Possible Investor Rights" [http://bit.ly/2v0euGp].

imposible una lectura acabada y razonable de los documentos integrantes del contrato inteligente. Esto hizo que los inversores simplemente estuvieran aceptando los términos impuestos por la organización autónoma descentralizada o sus creadores, dependiendo de si se consideraba que The DAO era sujeto de derecho o no.

5. *Smart contracts* en el Derecho argentino

Habiendo analizado el concepto de contrato inteligente tanto desde un punto de vista técnico como desde el Derecho comparado, corresponde pasar a reflexionar sobre su utilización en el ámbito local y determinar una aproximación desde el Derecho argentino. En este sentido, consideramos esencial reparar en el hecho de que este análisis se realizará asumiendo la existencia de una relación jurídica instrumentada mediante un contrato inteligente. Es decir, estaremos parados en una situación donde en el *smart contract* se ha codificado un contrato legal, es decir, la instrumentación del acuerdo será realizada mediante software. Para nuestro análisis, tampoco vamos a considerar una situación que implique una disminución en las capacidades para contratar o en la existencia de algún elemento que implique una diferencia entre la posición de las partes a la hora de contratar, es decir, partiremos de un supuesto de plena capacidad en materia contractual y paridad entre las partes de la relación. Sin perjuicio de ello, haremos una reflexión sobre la existencia de límites, como por ejemplo que el texto de un acuerdo constituya cláusulas predispuestas, o que exista la aplicación de una normativa de orden público que busque proteger a una de las partes.

Nuestro análisis se concentrará, principalmente, en el estudio de la forma de los contratos. Asumiremos que el resto de los elementos del contrato (causa, objeto, etc.) son legales y están presentes. Es decir, analizaremos si es posible instrumentar un contrato mediante software, como se pretende hacer con los contratos inteligentes.

Nuestro punto de partida, entonces, será en una primera instancia el artículo 958 del CCyCN. Dicho artículo recepta lo establecido en el anterior Código Civil de la Nación en su artículo 1197, que consagraba la llamada "autonomía de la voluntad", es decir, la potestad

que tienen las partes de un contrato a fijar entre sí los derechos y las obligaciones que estas estimen pertinentes al caso de igual manera y con la misma fuerza que lo hace el Estado con relación a las partes en forma individual por intermedio de la ley. La anterior redacción de este principio nos parece más ilustrativa de esta idea ya que decía que "las convenciones hechas en los contratos forman para las partes una regla a la cual deben someterse como a la ley misma". Desde ya que esta idea original prevista por Dalmacio Vélez Sarsfield en su código respondía a los ideales políticos de la época y la concepción que tenía el anterior Código Civil de plenitud civil de las personas para obligarse, salvo una situación excepcional de incapacidad; asimismo, este principio de la autonomía de la voluntad respondía a los principios fundacionales de la República Argentina, hoy ligeramente olvidados, de limitación en los avances del Estado sobre la voluntad de los particulares, los cuales están previstos en nuestro ordenamiento jurídico desde la sanción de la Constitución Nacional y su incorporación en los artículos 14 y 19. La actual redacción del CCyCN establece que, en principio, las partes son libres de contratar pero solo pueden hacerlo dentro de lo permitido por la ley, el orden público, la moral y las buenas costumbres. Es decir, sin perjuicio de que bajo el viejo Código Civil de Vélez también se seguía la misma lógica mediante el artículo 953 que refería a los actos jurídicos, en el CCyCN las partes pueden realizar todo tipo de actos jurídicos dentro del marco que les permite la legislación.[18]

En principio, entendemos que un contrato inteligente no es contrario a la ley, el orden público, la moral o las buenas costumbres, esencialmente porque no hay norma que prohíba el uso de estos instrumentos para la celebración e instrumentación de un contrato. Incluso debemos considerar que existe una política de digitalización de la vida comercial apoyada por diversas normas, desde el CCyCN hasta las leyes de simplificación y desburocratización, pasando por el impulso al sector *fintech* por parte del Banco Central de la República Argentina. Entendemos que las limitaciones a los contratos inteligentes estarán dadas por aquellos

[18] Cfr. Stiglitz, Rubén S.: "Un nuevo orden contractual en el Código Civil y Comercial de la Nación", *LL*, 2014-E, p. 1.332.

casos en los que el tipo de relación jurídica que se pretenda instrumentar mediante estos exija el cumplimiento de ciertas formalidades bajo pena de nulidad del acto subyacente o simplemente configurando una promesa de realizar el acto en cuestión con las formalidades requeridas.

Por lo tanto, si se logra instrumentar, siempre que el tipo de contrato lo permita, en el software el consentimiento de las partes para crear, regular, modificar, transferir o extinguir una relación jurídica, el *smart contract* será un contrato en sentido legal. Caso contrario, entendemos que el *smart contract* simplemente será una parte más de un contrato que usa al software como un mecanismo para la realización de ciertos actos en nombre de las partes del contrato.

Al respecto, recordamos que los contratos, conforme el CCyCN, pueden ser clasificados en formales y no formales, tal como señala el artículo 969. En los contratos formales, la normativa puede que exija la forma como condición de validez del acto o bien puede que la falta de formalidad no nulifique el acto sino que simplemente supedite su validez al otorgamiento de las formas requeridas quedando en cabeza de las partes una obligación de realizar tal acto, siendo ello exigible ante la justicia tal como prescribe el artículo 1.018 del CCyCN. Por otro lado, los contratos no formales son aquellos en los que la formalidad simplemente constituye un medio de prueba de la relación contractual instrumentada mediante el contrato. Respecto de la forma, como elemento de los contratos, el CCyCN establece el principio de libertad de formas a menos que exista un requisito legal en tal sentido, como bien se desprende del artículo 1.015.

Realizadas estas aclaraciones, corresponde pasar a determinar si el uso de un soporte electrónico es suficiente para cumplimentar con el requisito de la escritura que suelen exigir varios de los contratos previstos en el CCyCN. A estos efectos, debemos remitirnos a la parte general del CCyCN donde se regula la forma de los actos jurídicos en general, la cual sigue el mismo espíritu de la autonomía de la voluntad, conforme se establece en el artículo 284. Ahora bien, cuando se pasa a analizar cómo puede materializarse la forma escrita, el CCyCN 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*"[19]. Esta última parte nos permite concluir que los *smarts contracts* podrían ser contratos en sentido legal puesto que la instrumentación mediante software es viable.

Aclarado que un contrato puede instrumentarse mediante software, cabe analizar cómo se expresa la voluntad en este formato. En este sentido, el artículo 288 del CCyCN establece que la "firma prueba la autoría de la declaración de voluntad expresada en el texto al cual corresponde", la pregunta que tenemos que hacernos consecuentemente es cómo debería ser esta firma en los *smart contracts*. La respuesta a esta pregunta podemos encontrarla, en principio, en la parte final del artículo que estamos reseñando, el cual sostiene que "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".

A priori, parecería que este requisito de firma solo podría ser satisfecho mediante el uso de firma digital. La cuestión no resulta menor porque, de estar frente a un instrumento sin firma, tendríamos un instrumento particular no firmado, el cual, al no contener esta expresión de la voluntad, no nos permitiría decir que estamos frente a un instrumento que contiene un contrato. Esta redacción que tiene el CCyCN ha sido objeto de discusión por la doctrina en diversos artículos. Previo a la sanción del CCyCN, nuestro país ya contaba con la Ley N.º 25.065 (Ley de Firma Digital o LFD, en forma indistinta), la cual preveía dos tipos de firmas en soportes tecnológicos: la firma digital y la firma electrónica. La discusión doctrinaria luego de la sanción del CCyCN era si este había derogado la LFD o si las estipulaciones de esta norma seguían vigentes pero debían ser interpretadas al nuevo texto.

Al respecto, recordamos los artículos 2 y 5 de la LFD, que definen los conceptos de firma digital y firma electronica. Según la LFD, por firma digital "se entiende […] al resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose esta bajo su absoluto con-

[19] Nota del autor: el destacado es mío.

trol". Por otro lado, bajo el concepto de firma electrónica "se entiende […] al conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizado por el signatario como su medio de identificación, que carezca de alguno de los requisitos legales para ser considerada firma digital".

Estos tipos de firmas se diferencian por los requisitos que demandan y los efectos que producen. En este sentido, las firmas digitales hacen uso de un certificado digital emitido por un certificador habilitado por la autoridad de aplicación, previo proceso de validación de identidad; estos certificados tienen un término de validez para su uso. De reunirse estos requisitos, la firma digital goza de una presunción de autoría e integridad, elementos que recogió el CCyCN. Es por ello que la doctrina sostiene que la LFD ha dotado a la firma digital de efectos superiores a aquellos de la firma ológrafa, dado que la firma digital y el documento digital gozan de plena fe hasta que se demuestre lo contrario[20]. Respecto de las firmas electrónicas, estas son reconocidas por el artículo 5 de la LFD. En los casos en los que un firmante de un documento electrónico emplea cualquier forma para identificarse, aquello constituirá una firma electrónica. Cuando la firma no cumpla con los requisitos de validez para ser considerada "firma digital", entonces será reputada como "firma electrónica". La firma electrónica no goza de las presunciones de las que sí goza la firma digital. En razón de ello, de ser desconocida la firma electrónica, deberán probarse su autoría e integridad mediante diferentes elementos probatorias, principalmente un pericia informática, en sede judicial.

Con la sanción del CCyCN y la redacción del artículo 288, ciertos sectores de la doctrina sostuvieron que el requisito de la firma solo se cumple si se firma digitalmente, siendo totalmente inválida la firma electrónica para expresa la voluntad de una persona[21]. Sin embargo, y siguiendo a Mora, consideramos que "a todo evento, debe aclararse que la admisión de que la firma electrónica no es equiparable a firma ológrafa de ninguna manera significa que la firma electrónica no sirva para acreditar la manifestación de voluntad, o que no sirva para resistir rechazos de autoría e inte-

[20] Cfr. Mora, Santiago J.: "Documento digital, firma electrónica y digital", 2014-A, *LL*, p. 502.
[21] Cfr. Granero, Horacio R.: "Validez —o no— de los documentos electrónicos sin firma digital en el Código Civil y Comercial de la Nación", *elDial*, DC1FAD.

gridad. La firma electrónica va a servir para formalizar la manifestación de voluntad de cualquier persona en la medida en que ninguna norma exija una formalidad específica para ello (como por ejemplo, una firma ológrafa exclusivamente); y la firma electrónica va a servir para resistir rechazos de autoría e integridad en la medida en que la tecnología que utilice la firma electrónica en cuestión sea lo suficientemente avanzada para ello (no todas las firmas electrónicas van a lograrlo)"[22][23]. Es decir, al no haber sido derogada expresamente la LFD cuando fue sancionado el CCyCN, a diferencia de lo que sí ha ocurrido con otras normas que regulaban materias que también eran contempladas por el CCyCN, solo podemos concluir que el régimen de la LFD, incluyendo las disposiciones sobre firma electrónica, sigue plenamente vigente y, en cualquier caso, solo actúa como norma reglamentaria sobre esa firma digital de la que habla el CCyCN. Sobre esto último, y compartiendo el criterio de Mora, creemos que el CCyCN permite la asimilación de las firmas electrónicas avanzadas —categoría reconocida por la Unión Europea— a las firmas digitales, y dotando a estas de los mismos beneficios que las segundas.

En caso de desconocimiento de la firma electrónica, es necesario demostrar su autoría por cualquier medio, de acuerdo con lo previsto por el artículo 314 del CCyCN que prescribe: "[…] La autoría de la firma puede probarse por cualquier medio […]". Contar con otros elementos probatorios de la relación contractual que sean convincentes para el juez es de suma importancia para el caso dado que, por aplicación del artículo 319 del CCyCN, el valor probatorio de estos elementos será apreciado por este para determinar la congruencia entre lo sucedido y lo 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.

La cuestión sobre el uso de firmas electrónicas o digitales no es menor

[22] Mora, Santiago, "Análisis de las disposiciones sobre firmas digitales, firmas electrónicas y documentos digitales en el acceso al crédito y la inclusión financiera. Varios aciertos y un desacierto", LL, Suplemento Especial "Decreto de desburocratización y simplificación: Impacto en el mundo empresarial y en la gestión pública", Pág. 214.

[23] En idéntico sentido también podemos citar a Guini, Leonor, "Aspectos jurídicos del mercado de firma digital en Argentina. A propósito del nuevo Código Civil y Comercial", *RDYNT – Revista Derecho y Nuevas Tecnologías*, número 1, 2017, p. 77 y ss.

puesto que la gran mayoría de las plataformas usadas para contratos inteligentes que existen hoy hacen uso de firmas electrónicas más o menos complejas desde el punto de vista técnico.

Para la formación del consentimiento es necesaria la concurrencia de una oferta y una aceptación. Los requisitos de forma de la oferta y la aceptación seguirán los requisitos formales que tenga el contrato para considerar que ha sido perfeccionado con lo cual, si no hay mayores obstáculos respecto del medio sobre el cual deben instrumentarse sea el soporte electrónico o digital, según el caso, será plenamente valido.

Por lo tanto, podemos concluir que, en la medida en que no exista una norma que limite la posibilidad de instrumentar un contrato usando medios electrónicos que no hagan uso de firmas digitales, un *smart contract* podría ser considerado un contrato en los términos del artículo 957 del CCyCN. En el caso de que el *smart contract* no pueda ser considerado como un contrato, tenemos tres posibilidades: *(i)* considerarlo como una promesa de otorgar el contrato legal, conforme lo establecido en artículo 1.018 CCyCN; *(ii)* simplemente considerarlo como una herramienta utilizada por las partes para instrumentar y automatizar ciertos aspectos de la relación jurídica subyacente; o *(iii)* tomar este contrato inteligente como un principio de prueba instrumental por revestir el mismo el carácter, en este caso, de instrumento privado no firmado o firmado, en consonancia con lo prescripto por el artículo 1.020 del CCyCN.

A modo de ejemplo, un *smart contract* típico sería una transferencia de *tokens* tras el paso de cierto tiempo a cambio de otra cantidad determinada de *tokens* en un *exchange* descentralizado; recordemos que estos son clasificados como bienes[24] en los términos de los artículos 15 y 16 del CCyCN. En particular, cabe entender a los *tokens*, con independencia de la red a la que pertenecen, como el derecho a realizar una cantidad determinada de actos, en función de la cantidad de *tokens* que se tengan y las

[24] Si bien la naturaleza jurídica de los tokens está en amplia discusión en todo el mundo actualmente y es necesario determinar el comportamiento concreto del token en cada red blockchain para clasificarlo como "payment token", "utility token" o "security token", a fin de darle un tratamiento jurídico apropiado y acorde con su funcionalidad económica, una aproximación genérica permite adoptar la categoría de bienes a los efectos de este artículo. Para mayor información sobre el debate en torno a los tokens se puede recurrir a las publicaciones de Cristina Carrascosa en https://medium.com/@carrascosa.cobos.

reglas de comportamiento de la red a la que pertenecen y cuyo valor está fijado por el mercado sin perjuicio de la facultad de las partes de fijarlo de así desearlo. En particular, puede considerarse a estas redes como un contrato entre todos sus participantes quienes voluntariamente aceptan formar parte de ella en alguna de las redes típicas de las cadenas de bloques (mineros, oráculos, meros participantes, etc.). Al transferir todos los *tokens* o una parte de ellos, el transmitente de estos está cediendo, total o parcialmente, su posición en este contrato para realizar estos actos.

En virtud de ello, es posible considerar la transferencia de *tokens* como una cesión de posición contractual, la cual se encuentra regulada en los artículos 1.636 y siguientes del CCyCN. Dado que la cesión de posición contractual es un subtipo de cesión de derechos, cabe aplicar también las normas relativas a cesión de derechos. En lo que hace a la forma de este tipo de acuerdos, el artículo 1.618 establece que, salvo los casos allí indicados, el contrato debe hacerse por escrito. He aquí donde la discusión que hemos planteado antes toma relevancia. Siguiendo con el criterio planteado más arriba, la forma escrita se encontraría satisfecha mediante la utilización de firmas y soportes electrónicos.

Tal como adelantamos, este análisis parte del supuesto de paridad entre las partes, situación que no suele darse en la práctica por diferentes motivos que no serán objeto de este análisis. Estas disparidades entre las partes dan lugar a limitaciones de las voluntades de las partes y al principio de autonomía de la voluntad, en línea con lo prescripto por el artículo 958 del CCyCN. Los límites en cuestión son las previsiones sobre contratación por cláusulas predispuestas y sobre contratación con consumidores.

El primer tipo de limitaciones encuentra su razón en el componente tecnológico y el hecho de que la práctica actual en materia de *smart contracts* denota la imposición de software de una parte a la otra. Es decir, por lo general una de las partes es quien impone a la otra el software que receptará los derechos y obligaciones pactados entre las partes sin dar posibilidad de discutir la redacción o programación del contrato inteligente. Como consecuencia de ello, es posible considerar a estos contratos inteligentes como contratos con cláusulas predispuestas en los términos de los artículos 984 a 989. Esta categorización nos trae dos problemas: el primero sería que si el texto del contrato está circunscripto al código, po-

dría haber un incumplimiento del párrafo 2 del artículo 985 por la falta de claridad y facilidad de lectura; y segundo, estaría abierta la posibilidad de la declaración de nulidad de ciertas cláusulas que sean consideradas como abusivas. Al respecto de estos problemas, un juez podría estimar que: *(i)* el contrato no es *smart contract* por no reunir estos elementos de claridad y transparencia; y *(ii)* debe integrar el contrato con elementos adicionales fuera del código, tornando todo el esfuerzo de autosuficiencia del contrato inteligente en una actividad superflua. En particular, el problema con la integración judicial del contrato inteligente radica en cómo hacer que esta orden judicial sea seguida por el protocolo que gobierna al contrato inteligente.

Por otro lado, la segunda gran barrera frente a la cual se topan los contratos inteligentes es la normativa protectora del consumidor, tanto en el CCyCN como en la Ley 24.240 y sus modificatorias. Si bien estas normas tienden a defender a la parte débil, de forma muy similar al régimen reseñado en el párrafo anterior, es cierto que también es una normativa que ha receptado la plena validez de los medios electrónicos para la contratación. Al respecto, creemos que cumpliendo con los deberes de información previstos tanto en el artículo 4 de la Ley 24.240 como en el 1.110 del CCyCN, sobre las características e implicancias del uso de un *smart contract* así como también si se evita introducir cualquier cláusula que resulte lesiva para el consumidor, el contrato inteligente tendría plena validez.

Recordemos que la contratación por medios está permitida en la medida en que el consumidor sea informado sobre su funcionamiento. Toda esta información, según la última reforma a la Ley 24.240, puede estar en soporte electrónico. Claramente aquí el desafío ya no será jurídico sino práctico para lograr la educación del consumidor sobre el uso de estas plataformas. Cabe recordar el reciente fallo "Kosten"[25] de la Cámara Nacional de Apelaciones en lo Comercial que se ha pronunciado sobre la plena validez de los términos y condiciones de una plataforma como medio para informar a un consumidor sobre el funcionamiento de esta; sin embargo, debe repararse en el hecho de que el código no es lo mismo que el texto plano, como suelen estar redactados

[25] Cámara Nacional de Apelaciones en lo Comercial, Sala D, "Kosten, Esteban c/ Mercado Libre SRL s/ ordinario", 22 de marzo de 2018 [https://bit.ly/2K6GoWd].

los términos y condiciones de una plataforma, a pesar de ser ambos, en última instancia, software.

Uno de los temas de debate por la doctrina es el rol de los abogados y la responsabilidad civil derivada de una mala praxis[26]. Dado que la redacción de los contratos pasaría a hacerse con código y no con un lenguaje humano, los abogados que programan tendrán doble responsabilidad: por un lado, responsabilidad por el asesoramiento jurídico sobre el negocio en cuestión, y por otro lado, responsabilidad por la programación de software que debe cumplir cierta finalidad. Es decir, tendrán a su cargo una obligación de medios y otra de resultado, respectivamente. Por su parte, creemos que muchos programadores estarán tentados a redactar estos contratos y podrían verse dando asesoramiento legal sin habilitación para ello. Lo más sensato, seguramente, sea la conformación de equipos de trabajo multiprofesionales para atender las diferentes aristas del desafío.

No solo los regímenes de contratos con cláusulas predispuestas y de protección al consumidor deben ser atendidos. Si bien estos campos, que limitan la autonomía de la voluntad, son los principales por los condicionamientos sobre las formas, también hay muchos otros ámbitos donde estos contratos inteligentes pueden toparse con límites. Tal como señalan Wright y De Filippi, el mundo financiero, donde se habla mucho del uso de *smart contracts*, suele presentar la existencia de partes débiles frente a las cuales un regulador podría prohibir el uso de estos instrumentos para velar por el inversor promedio, por ejemplo. En este, una de las primeras aplicaciones de contratos inteligentes —las *initial coin offerings* (ICO)— se ha visto reducida a ser ofrecida solo a inversores calificados para evitar cumplir con cargas regulatorias. De esta forma se pierde el sentido que motivó la existencia de las ICO —permiten el acceso masivo del público a financiar un *startup*— por la reducción y queda, nuevamente, el acceso a esquemas de inversión más riesgosos solo para aquellos que denotan "profesionalidad" o "experiencia" en la materia.

Como vemos, si bien muchos de los problemas o desafíos jurídicos

[26] Wright, Aaron, & Primavera De Filippi, "Decentralized Blockchain Technology and the Rise of Lex Cryptographia", p. 24 [https://bit.ly/2LRPHhH].

que plantean los contratos inteligentes pueden ser resueltos con los elementos normativos que tenemos hoy, también existen cuestiones para las cuales el Derecho no puede dar una respuesta o solución que sea práctica o concreta y no implique razonar o pensar en prohibiciones o limitaciones. En este sentido, Wright y De Filippi apuntan a que estas cuestiones podrían ser resueltas mediante un conjunto normativo específico que siga el espíritu que tuvo en su génesis la *lex mercatoria*: la *lex cryptographia*. A su criterio, la *lex cryptographia* actúa como una segunda instancia de la ley informática, la cual regula las relaciones jurídicas sobre la tecnología mediante documentos técnicos como el código. Los autores consideran que la *lex cryptographia* será el elemento de la "arquitectura", según la clasificación de modos de regulación de Internet propuesto por Lessig, que tendrá peso sobre esta nueva realidad.

6. Conclusiones

La tecnología nos ha proporcionado y nos seguirá proporcionando elementos para hacer más eficientes nuestras relaciones jurídicas. Sin embargo, la validez legal de estas puede y será cuestionada por algunos actores jurídicos. Frente a ello, tenemos la obligación de estudiar cómo integrar nuestro marco normativo para darles recepción a los nuevos institutos que la tecnología pueda darnos, en particular aquellas herramientas que actúen como medios alternativos para la resolución de controversias.

Como hemos podido analizar siguiendo los comentarios de juristas de diferentes jurisdicciones y el comentario a los contratos inteligentes realizado a la luz de la normativa local, podemos concluir que los *smart contracts*, tal como funcionan hoy en día y se interrelacionan con el sistema jurídico actual, son formas que pueden revestir los contratos. Habrá casos en los que la instrumentación mediante software será posible, mientras que en otras situaciones ello no podrá ser así y necesitaremos usar otros elementos para conformar el contrato, todo ello sin dejar de lado la posibilidad de tomar al contrato inteligente como un principio de prueba por escrito o una promesa de dar el instrumento correspondiente para celebrar. También será necesario reparar en la efectiva utilidad que tiene el contrato inteligente en aquella situación; si estamos en una situa-

ción en la que el uso de software como instrumentación no tiene la fuerza suficiencia para satisfacer el requisito de forma y debemos recurrir a las "viejas" formas, poco sentido tiene usar un *smart contract*. Muchas de sus funcionalidades tendrán plena vigencia en relaciones paritarias, pero no así cuando se topen con marcos normativos que tienden a proteger a alguna de las partes involucradas en la transacción subyacente. Asimismo, siguiendo lo reseñado por Raskin, si bien la puerta de la revisión judicial siempre estará abierta, su utilidad dependerá de la fortaleza del contrato para admitir la intervención judicial.

Estamos en una época de transición y de cambios tecnológicos con impacto directo en las instituciones jurídicas y su eficacia para dar respuesta a estos problemas. El caso "The DAO" ha sido un claro ejemplo de ello; si bien un reclamo por ese evento no ha sido judicializado, solo las preguntas que nos plantea nos hacen poner de manifiesto las insuficiencias del sistema jurídico para resolver los problemas planteados. Creemos que la voluntad de las partes y el principio de la autonomía de la voluntad cobran un nuevo sentido en este contexto. Así como en aquel caso fueron las personas quienes eligieron entre ellas cómo resolver el problema y solucionar sus conflictos en forma privada, estimamos que este nuevo orden jurídico, descripto brevemente por Wright y De Filippi,[27] resolverá los problemas tal como lo hicieron los mercaderes con la *lex mercatoria* durante la Edad Media.

No debemos perder de vista que, mientras ello sea posible, el principio de la autonomía de voluntad sigue plenamente vigente y no existe nadie mejor que las partes para definir cómo va a ser la relación jurídica que estas crean con relación a determinados derechos. El derecho particular que puedan crear los particulares será sensiblemente superior a una decisión dispuesta por el Estado en forma general. Asimismo, no solo las partes son las más idóneas para determinar qué norma regirá sus relaciones, sino que también son estas las más capacitadas para decidir cómo resolver sus conflictos que surjan de estas relaciones. Hoy las partes ya tienen las herramientas técnicas para ordenar sus relaciones y los efectos

[27] La noción de *lex cryptographia* es ampliada en el libro de Wright, Aaron De Filippi, Primavera, "Blockchain and the Law: The Rule of Code", Harvard University Press, 2018.

de estas sin la necesidad de recurrir a terceros de confianza o al Estado para efectivizar esos derechos y obligaciones. No es necesario que el Estado reconozca su validez de estas herramientas técnicas; los contratos inteligentes son válidos por nacer de la misma voluntad de las partes, fuente principal y por excelencia para la creación de derechos y obligaciones.

El Convenio sobre Ciberdelito del Consejo de Europa y su incorporación al ordenamiento interno argentino

por Carla Delle Donne

Palabras clave: delitos informáticos, Convenio sobre Ciberdelincuencia, ratificación, armonización, Código Penal, Código Procesal Penal, adecuación normativa, Ley N.º 27.411.

1. Introducción

El desarrollo ininterrumpido de la tecnología de las últimas décadas que trajo como resultado la evolución de los modos en que nos comunicamos y llevamos a cabo actos de la vida cotidiana, constituye uno de los fenómenos más representativos de la sociedad globalizada. La trasformación sociopolítica, cultural y económica de la humanidad generada por la influencia de informática conlleva innumerables aspectos positivos. Sin embargo, frente a los beneficios ilimitados que ofrece un dispositivo electrónico conectado al servicio de Internet —la red que hoy nos conecta a todos—, el ciberespacio se presenta como ámbito propicio para la delincuencia informática.

En ese contexto, y ante la necesidad de definir nuevos intereses que deben ser protegidos por la ley penal y de contar con legislación procesal que permita llevar adelante investigaciones efectivas para luchar contra los ciberdelitos que amenazan a toda la comunidad internacional, se sancionó el Convenio sobre Ciberdelito[1] (Convenio sobre la Ciberdelincuencia o Convenio de Budapest, en adelante "el convenio"). Ese primer tratado internacional se abrió a la firma el 23 de noviembre de 2001 en la ciudad de Budapest, Hungría, y entró en vigencia el 1 de julio de 2004 tras alcanzar la ratificación de cinco Estados, tres de los cuales, según es-

[1] La la traducción oficial argentina denomina al instrumento internacional como "Convenio sobre Ciberdelito". Las versiones oficiales del convenio se encuentran redactadas únicamente en idioma inglés y francés. El sitio oficial del Consejo de Europa cuenta con una versión en español cuya traducción y denominación del tratado no coincide con la traducción oficial efectuada en nuestro país. La traducción del Consejo de Europa lo denomina Convenio sobre la Ciberdelincuencia.

tablece el propio convenio en el artículo 36, tenían que ser Estados parte del Consejo de Europa. Desde ese entonces, el convenio se erige como el único tratado internacional sobre la materia en el ámbito del Derecho internacional penal.

La República Argentina, luego de largos años de negociaciones —tanto en el ámbito internacional como en el nacional— que involucraron el cumplimiento del procedimiento especial de adhesión que establece ese instrumento para terceros Estados,[2] ratificó el convenio mediante la aprobación de la Ley N.º 27.411, publicada en el Boletín Oficial el 15 de diciembre de 2017. El depósito del instrumento de ratificación se realizó el 5 de junio de 2018 ante el secretario general del Consejo de Europa y, de ese modo, la República Argentina prestó formalmente su consentimiento en obligarse por las disposiciones del tratado, circunstancia que marca el inicio de una nueva etapa de armonización de la legislación penal y procesal penal interna.

A los fines de examinar el proceso de incorporación del convenio a nuestro ordenamiento interno, en primer lugar, analizaré el marco institucional en el que se sancionó: el Consejo de Europa. En segundo término, examinaré el mecanismo especial de adhesión que prevé el artículo 37 para los terceros Estados que no negociaron sus términos para, luego, estudiar los argumentos a favor y en contra de la universalización de un convenio que, inicialmente, solo pudieron firmar los Estados que participaron en la adopción y aprobación del texto. En cuarto lugar, reseñaré someramente las distintas partes del convenio, sus disposiciones y, en particular, las reservas que admite. Finalizaré con el análisis del proceso interno de ratificación y la sanción de la Ley N.º 27.411 para cuyos fines me centraré en el examen en las reservas efectuadas y las lagunas normativas que se generan en nuestra legislación a la luz del estudio comparativo del convenio con el Código Penal (CP) y el Código Procesal Penal de la Nación (CPPN) vigente.

[2] Según lo dispone el artículo 2.h de la Convención de Viena sobre derecho de los tratados, se entiende por "tercer Estado" al Estado que no es parte en el tratado.

2. El Consejo de Europa y el Convenio sobre la Ciberdelincuencia

2.1. Marco institucional, Estados contratantes y entrada en vigencia

El Convenio sobre la Ciberdelincuencia que se abrió a la firma el 23 de noviembre de 2001 en Budapest, Hungría, tal como lo indica su informe explicativo, tuvo sus orígenes en los trabajos preparatorios iniciados en 1996 por disposición del Comité Europeo en el marco del Consejo de Europa.

La diferenciación institucional como punto de partir del análisis resulta a todas luces relevante, porque la ratificación del convenio tiene implicancias no solo en la aplicación práctica del Derecho internacional sino también en las relaciones internacionales que se entablarán en el ámbito de esa organización internacional regional. Identificar al Consejo de Europa como marco institucional, entonces, permite analizar el contexto en el que se redactó y aprobó el convenio, identificar a los Estados que intervinieron en esa tarea y considerar las consecuencias institucionales que a nivel internacional puede generar el hecho de ser parte del instrumento regional europeo que dispone un mecanismo especial de adhesión.

El Consejo de Europa no es parte de la Unión Europea ni depende institucionalmente del Consejo Europeo ni del Consejo de la Unión Europea. El Consejo de Europa, el Consejo Europeo[3] y el Consejo de la Unión Europea[4] son instituciones diferentes y no deben confundirse. El Consejo de Europa tiene su sede en Estrasburgo, Francia, y es una organización internacional que se creó tras la finalización de la Segunda Guerra Mundial en el Tratado de Londres de 1949. Desde ese entonces, el Consejo de Europa está integrado por 47 Estados, entre los que se encuentran todos los Estados de Europa más Bielorrusia.

La negociación del texto del convenio y su adopción estuvo a cargo de los Estados que integran el Consejo de Europa y Estados Unidos de Norteamérica, Canadá, Japón y Sudáfrica. La intervención de esos cuatro Estados que no forman parte del Consejo de Europa motivó la inclu-

[3] El Consejo Europeo es una institución de la Unión Europea que integran los líderes de la Unión Europea con sede en Bruselas, Bélgica. Fue creado en 1974.

[4] El Consejo de la Unión Europea es también una institución de la Unión Europea que integran los ministros de cada Estado. Su sede se encuentra en Bruselas y fue creado en 1958.

sión de una disposición especial que estableció que solo aquellos Estados pueden revestir la calidad de Estados firmantes. En efecto, el artículo 36 establece que el convenio "está abierto a la firma de los Estados miembros del Consejo de Europa y de los Estados no miembros que hayan participado en su elaboración".

Con relación a la entrada en vigencia, el mismo artículo 36 prevé que el convenio solo entrará en vigencia cuando cinco Estados hayan firmado y ratificado, aceptado o aprobado —modo que depende de las formas de manifestación del consentimiento del Estado en obligarse por un tratado[5] previsto en la legislación interna de cada Estado—, siempre que tres de esos cinco Estados sean Estados parte del Consejo Europeo. Esa mayoría se alcanzó el 1 de julio de 2004, fecha en la que el convenio entró en vigor estableciéndose como el primer tratado internacional dirigido a combatir la delincuencia en línea. El estatus de ratificación, tal como surge de la información disponible en la página del Consejo de Europa relativa al tratado, al mes de agosto de 2018, indica que son 61 los Estados que ratificaron o adhirieron y cuatro los que firmaron únicamente.

2.2. El régimen de adhesión como forma de prestar en consentimiento en obligarse por el convenio

El convenio establece un régimen especial de adhesión para los Estados no parte del Consejo de Europa y que no participaron en la elaboración del texto en el artículo 37. Esa disposición estipula que los terceros Estados podrán manifestar su consentimiento en obligarse por el tratado mediante la adhesión, a partir de su entrada en vigencia, y siempre que reciban la invitación del Comité de Ministros del Consejo de Europa (en adelante, "el Comité"). La invitación puede extenderse por iniciativa propia del Comité o a través de la solicitud expresa del tercer Estado.

Sin embargo, la invitación no puede cursarse de manera automática y el Comité se encuentra doblemente condicionado para hacerlo. Por un lado, la decisión formal de invitación debe contar con el voto unánime

[5] Los modos previstos para la manifestación del consentimiento en obligarse por un tratado para los Estados sigue las formas establecidas en los artículos 11 y 14 de la Convención de Viena sobre Derecho de los Tratados.

de las dos terceras partes de los representantes de los Estados con derecho a formar parte del Comité. Si alcanza ese consenso, también debe consultar a los restantes Estados contratantes y obtener el consentimiento unánime de todos aquellos.

El informe explicativo del convenio expresa una razón determinante a los fines de justificar el hecho que los Estados europeos deben prestar su consentimiento para invitar a un Estado que no forma parte del Consejo de Europa y que no participó de la redacción del tratado al afirmar que "todos los Estados contratantes del convenio deben poder determinar con qué Estado no parte entablarán relaciones relativas al convenio"[6]. De ese modo, el convenio establece un modo de adhesión que requiere de un proceso de negociaciones diplomáticas especiales que trascienden aquellas que se dan habitualmente a los efectos de manifestar el consentimiento en obligarse por los términos de un tratado por parte de los Estados.

Una vez atravesado el proceso de adhesión, y ratificado o aprobado el tratado según sea el modo de incorporar el Derecho internacional al Derecho interno del tercer Estado, de conformidad con el último párrafo del artículo 37, el convenio entrará en vigencia "el primer día del mes siguiente a la expiración de un plazo de tres meses desde la fecha de depósito del instrumento de adhesión en poder del secretario general del Consejo de Europa".

2.3. ¿El convenio regional europeo o un convenio mundial nuevo?

Desde su entrada en vigencia el 1 de julio de 2004, el convenio se erige como un instrumento que aspira a alcanzar la universalidad[7]. La universalidad, tal como sucede con todos los regímenes jurídicos establecidos en tratados internacionales, es la expectativa de alcanzar la mayor cantidad de ratificaciones de los Estados que forman parte de la comunidad internacional[8]. Sin embargo, existe un debate en la comunidad in-

[6] Informe explicativo del convenio, párrafo 306.
[7] Ibídem.
[8] Un claro ejemplo que puede definirse como universal es el régimen jurídico contra el terrorismo. La universalidad no implica que todos los actos terroristas se encuentren definidos en

ternacional acerca de las ventajas y desventajas que representa la adhesión a un convenio regional europeo frente a la posibilidad de elaborar un instrumento internacional en el seno de la Organización de las Naciones Unidas (ONU) en cuya elaboración intervengan todos los Estados que la integran que atentarían contra el anhelo de universalidad.

En efecto, se ha cuestionado largamente en distintos foros internacionales que la falta de intervención en la elaboración de los términos del tratado internacional de todos los Estados que integran la comunidad internacional y el mecanismo especial de adhesión antes reseñado constituyen dos principales razones por las cuales los Estados no estarían de acuerdo en firmarlo, ratificarlo o aprobarlo.

Los Estados que sostienen esa posición definen al convenio como un instrumento de corte únicamente europeo y, por ese motivo, expresan que sería más adecuado contar con un tratado negociado en el seno de la ONU que sea más representativo de todas las regiones. En ese sentido, también señalan que en materia de tratados internacionales, el convenio establece un régimen especial de adhesión que sigue un mecanismo que si bien se ha establecido en otros instrumentos internacionales del Consejo de Europa, en materia de Derecho internacional público resulta novedosa para Estados que no siguen la tradición jurídica de esa organización. El motivo es claro: los tratados negociados en el seno de la ONU así como aquellos aprobados en el marco de la Organización de los Estados Americanos (OEA), no limitan o condicionan la posibilidad de los Estados parte de participar activamente en el proceso de elaboración y aprobación de los términos de los tratados internacionales, del modo en que lo hace el convenio. Por otra parte, los instrumentos internacionales aprobados en el seno de la ONU se encuentran abiertos a la firma de todos los Estados parte hayan o no participado en la elaboración del texto, adopción o aprobación, y no necesitan invitación para devenir en Estado parte del tratado internacional.

las dieciocho convenciones y protocolos dictados en el marco de la ONU que integran el régimen jurídico global, sino que tiene como objetivo que la mayor cantidad de Estados ratifiquen las convenciones y, de ese modo, ser más efectivos en la lucha contra el terrorismo pues las ratificaciones de todas las convenciones por parte de todos los Estados evitaría la existencia de *safe havens* para las organizaciones terroristas y los terroristas.

Las opiniones que se alzan en contra del convenio también destacan que el mecanismo de adhesión previsto en el artículo 37 es lento y que, tal como sucede con otros tratados internacionales, los Estados deberían poder manifestar su consentimiento en obligarse mediante la firma al tiempo que se adopta y aprueba el texto del tratado, en lugar de hacerlo tras su entrada en vigencia y sujeto a la decisión de los Estados contratantes que implica largos procesos de burocracia diplomática.

Otra de las críticas al convenio es aquella que señala que se trata de un convenio que estaría desactualizado porque los trabajos preparatorios comenzaron a elaborarse en 1996 y la redacción del texto data del año 2001. Los años que transcurrieron desde ese entonces no reflejarían la realidad de la criminalidad informática actual sino la clasificación de los delitos informáticos y las definiciones de conductas criminales que coinciden con el conocimiento de la criminalidad online de aquella época y que, en consecuencia, estarían desactualizadas con relación a la evolución de la temática en las casi dos décadas que transcurrieron desde la entrada en vigencia del convenio.

Por otro lado, los Estados que entienden que la ratificación o aprobación del presenta desventajas frente a un instrumento internacional más global también destacan que los estándares establecidos en ese instrumento solo fueron pensados para países europeos desarrollados que cuentan con las instituciones necesarias y el conocimiento especializado que se requiere para investigar y perseguir eficazmente este tipo de delincuencia. En ese sentido, cuestionan la efectiva aplicación de los términos del convenio al indicar que el convenio solo podría ser satisfactoriamente aplicado en los Estados parte que cuentan no solo con los medios suficientes para producir cambios inmediatos en las legislaciones internas a los efectos de armonizar la ley interna con las disposiciones del tratado internacional, sino también con la capacitación y el entrenamiento de las fuerzas de seguridad y los operadores judiciales que sea adecuado a la lucha de la ciberdelincuencia y las características especiales de investigación que presenta.

Sin embargo, si se evalúan comparativamente esas eventuales desventajas con las ventajas que representa para terceros Estados la adhesión a un régimen jurídico sobre la ciberdelincuencia vigente y que cuenta con una larga trayectoria de experiencia en su aplicación práctica, fácil se

advertirá que es notablemente más positivo alentar la adhesión al convenio que esperar el resultado de los trabajos preparatorios destinados a la posible elaboración de un nuevo tratado internacional de la ONU[9].

A los fines de justificar los méritos de ratificar el convenio, cabe señalar, en primer lugar, que el convenio es un tratado en vigor circunstancia que implica que los mecanismos de implementación se encuentran en funcionamiento desde larga data. Como consecuencia de ese hecho, los conocimientos adquiridos durante los diecisiete años que transcurrieron desde su entrada en vigencia sobre: la armonización normativa del Derecho interno en materia de Derecho sustantivo y procesal, la reforma institucional que involucra la creación de organismos, oficinas, fiscalías, divisiones y equipos de las fuerzas de seguridad, la capacitación de las fuerzas de seguridad, operadores de justicia, funcionarios del Estado encargados de la prevención, persecución y juzgamiento de los delitos informáticos, la articulación del sector público con el sector privado y la concienciación sobre la problemática de la ciberdelincuencia de la sociedad civil, constituyen un capital invalorable que puede ser aprovechado para encarar los desafíos que presenta la ciberdelincuencia en la actualidad y los que surgirán en el futuro.

Por otro lado, de los 193 Estados que integran el sistema de la ONU, 61 son Estados parte del convenio, otros siete han sido invitados a adherir. Y aunque resulta evidente que queda una largo camino para alcanzar la universalidad, existen numerosos terceros Estados que, aunque por regla general no tienen derechos u obligaciones con relación al convenio porque no adhirieron,[10] han utilizado al convenio como guía para modificar su legislación penal interna[11].

---

[9] Cabe señalar que en el marco de la ONU desde que la Asamblea General dictara la resolución 65/230 en el marco del 12.º Congreso de las Naciones Unidas sobre sobre prevención del delito y justicia penal que dispuso la creación de un grupo intergubernamental de expertos para que realice "un estudio exhaustivo del problema del delito cibernético y las respuestas de los Estados miembro, la comunidad internacional y el sector privado ante ese fenómeno, incluido el intercambio de información sobre legislación nacional, mejores prácticas, asistencia técnica y cooperación internacional, con miras a examinar opciones para fortalecer las actuales respuestas jurídicas o de otra índole ante el delito cibernético en los planos nacional e internacional y proponer otras nuevas", ese grupo se ha reunido en reiteradas ocasiones para cumplir únicamente con esos objetivos.

[10] Según lo dispone el artículo 34 de la Convención de Viena sobre Derecho de los Tratados.

[11] El caso de la República Argentina es un ejemplo significativo. Se pueden citar también los casos de Chile, Uruguay, República Dominicana y Brasil.

Asimismo, y por oposición al argumento que sostiene que el convenio es un tratado que no estaría actualizado, más allá del hecho que las conductas ilícitas que contempla abarcan un amplio abanico de delitos informáticos, el tratado contempla la posibilidad de enmendar sus términos según lo dispuesto en el artículo 44 que habilita a los Estados parte a sugerir enmiendas que "deberán ser comunicadas al secretario general del Consejo de Europa, a los Estados miembros del Consejo de Europa, a los Estados no parte del Consejo de Europa que hayan tomado parte en la elaboración del convenio así como a los Estados que se hayan adherido o que hayan sido invitado a adherirse conforme a lo dispuesto en el artículo 37".

Por otra parte, cierto es que los Estados también pueden incluir en sus legislaciones todos aquellos delitos que no estarían contemplados en el convenio, así como también pueden establecer reglas de procedimiento que eleven los estándares allí establecidos.

En esa línea argumental, cabe señalar que luego de la entrada en vigor del convenio, se aprobó el primer protocolo adicional relativo a la criminalización de actos de naturaleza racista o xenófoba cometidos por sistemas informáticos que fue abierto a la firma el 28 de enero de 2003 y se encuentra en vigencia desde el 1 de marzo de 2006. Asimismo, el 8 de junio de 2017 comenzaron los trabajos preparatorios para la elaboración de un nuevo protocolo adicional relativo a la recolección de evidencia digital en la nube que recién a principio de 2020 finalizaría con sus negociaciones. Esos protocolos permiten afirmar que el convenio cuenta con los mecanismos necesarios para adecuar sus términos a las realidades tecnológicas e incorporar otros delitos, porque, tal como expresara anteriormente, son los Estados parte los que determinarán la evolución del texto del convenio en vigencia.

Por otra parte, el texto del convenio responde al principio de neutralidad tecnológica. Ese principio establece que la descripción de los tipos penales y las medidas de prueba se realice en términos genéricos de modo tal que no se identifiquen con una única realidad tecnológica o la tecnología existente en el momento de la redacción. El cumplimiento de ese principio implica que el convenio aspira a tener una vigencia temporal extendida que no depende de los avances tecnológicos y los cambios en las modalidades de comisión de los delitos informáticos que se benefician con ese desarrollo. Es ese sentido, el informe explicativo del convenio

expresa que "el convenio utiliza un lenguaje neutro en cuanto a la tecnología de manera tal que los delitos contemplados en el derecho penal puedan aplicarse tanto a las tecnologías actuales como a las futuras".

Por otra parte, al ser un tratado internacional en plena vigencia, el convenio cuenta con mecanismos de cooperación internacional y asistencia legal mutua que están siendo aplicados y se encuentran en funcionamiento. Esa circunstancia indica mayor efectividad en investigaciones que tienen impacto transnacional y que es el resultado de la interacción generada a lo largo de los años.

Por último, corresponde destacar que, al asumir las obligaciones internacionales que aparejan la ratificación o adhesión de un convenio vigente, se fortalece la seguridad jurídica del propio régimen en el ámbito internacional. Es que no puede dejar de señalarse que los procesos de negociaciones, elaboración y aprobación de un nuevo tratado internacional podrían crear riesgos a la vigencia del único régimen de lucha contra la delincuencia informática que atentaría contra todos los esfuerzos dedicados a la puesta en funcionamiento y efectiva aplicación del convenio. La posible existencia de un nuevo tratado internacional interrumpiría las reformas legislativas e institucionales en curso de los Estados parte o de los Estados en proceso de adhesión al convenio; tendría estándares más básicos en términos de preservación y recolección de prueba digital y, en consecuencia, de cooperación internacional con el objetivo de reducir las invocadas asimetrías existentes entre los Estados; y, por último, podría generar resultar perjudicial para el normal desarrollo normativo del convenio que, desde la aprobación del texto, ya cuenta con un protocolo adicional y otro en vías de preparación.

2.4. El Convenio sobre Ciberdelito

2.4.1. Normas de Derecho sustantivo: clasificación de delitos informáticos y delitos informáticos

El convenio establece en el preámbulo que los delitos informáticos son aquellos delitos que atentan contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, de las redes y de los datos, así como el uso fraudulento de esos sistemas, redes y datos. De esa

manera, el tratado establece una clasificación que, si bien no define el concepto de delitos informáticos, propone una categorización que constituyó tanto el puntapié inicial de la conceptualización de ese tipo de criminalidad[12] como el estándar mínimo de tipificación.

El capítulo II, sección 1, título 1 del instrumento internacional establece que los Estados parte deberán adecuar su normativa interna a los fines de tipificar delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos. La particularidad de esa primera clasificación es que nuclea todos los delitos cuyo medio para cometer el accionar ilícito involucra la intervención de un dispositivo informático y el objeto y el fin del delito son datos informáticos o el propio sistema informático.

En esa primera clasificación se incluyen: a) el acceso ilegítimo a un sistema informático, la interceptación ilícita de datos informáticos, los ataques contra la integridad de datos informáticos que a su vez comprenden conductas de dañar, borrar, deteriorar, alterar o suprimir datos informáticos (artículos 2, 3 y 4); b) los ataques contra la integridad de los sistemas informáticos a través de accesos ilegítimos cometidos mediante la introducción, la transmisión, el daño, el borrado, el deterioro, la alteración o la supresión de datos informáticos (artículo 5); c) el abuso de dispositivos para cometer los delitos antes mencionados (artículo 6).

En la segunda categoría de delitos informáticos el convenio agrupa una serie de delitos comunes que se comenten mediante la utilización de un sistema informático. El título 2 sobre delito informáticos recomienda la tipificación de: a) la falsificación informática que comprende toda falsificación de documentos digitales y protege la seguridad y fiabilidad de los datos electrónicos (artículo 7); b) el fraude informático que incluye las estafas cometidas con tarjetas de crédito o débito —denominado también *carding*— (artículo 8). El título 3 sobre delitos informáticos que protegen el contenido insta a los Estados parte a tipificar delitos relativos

[12] En el "Comprehensive study on cybercrime" (*draft*), publicado en febrero de 2013, la Oficina de las Naciones Unidas contra Droga y el Delito afirma que no existe una única definición del concepto delitos informáticos y que la ausencia de esa definición solo importa a los fines de la cooperación internacional porque es difícil que todos los tipos penales puedan quedar comprendidos bajo un solo concepto que abarque a todos los delitos informáticos, y que aún de existir sería una definición artificial.

a la comisión de delitos vinculados con la producción, el ofrecimiento, la puesta a disposición, la difusión o transmisión, la obtención para sí o para terceros y la tenencia de material digital de abuso sexual de los menores de edad por medios informáticos que el convenio denomina "pornografía infantil", tal como se refería a ese delito en la época de la aprobación del texto del convenio[13] (artículo 9). Por último, el título 4 recomienda la tipificación de los delitos vinculados a las infracciones contra la propiedad intelectual y los derechos afines que tiene como objetivo primordial proteger los derechos de autor y los derechos conexos (artículo 10).

El convenio establece que todos los delitos previstos son delitos dolosos, que los artículos 3 a 5, 7, 8, 9.1.a y 9.1.c admiten la tentativa (artículo 11.2) y que no solo debe atribuirse responsabilidad penal a los autores y coautores sino que también los Estados deben aplicar sanciones penales a los partícipes (artículo 11.1) y las personas jurídicas cuando el delito sea cometido por una persona física (artículo 12).

2.4.2. Normas de Derecho procesal

El capítulo II, sección 1, sección 2 dispone las reglas de Derecho procesal que deben adoptar las partes para investigar y perseguir eficazmente los delitos informáticos previstos en el convenio o cualquier otro delito cometido a través de un sistema informático así como recopilar pruebas informáticas de cualquier tipo de delito (artículo 14).

El estándar mínimo de normas procesales que prevé el convenio y que, a la luz del principio de proporcionalidad, deben asegurar el respeto de los derechos humanos (artículo 15) incluyen: a) la conservación rápida de datos informáticos almacenados en el marco de una investigación (artículo 16); b) la conservación y divulgación inme-

[13] Sobre la definición del tipo penal como pornografía infantil, cabe señalar que no es correcta porque referirse a los abusos sexuales como material pornográfico de menores legitima el concepto de pornografía infantil como una categoría o clase de pornografía en todos los casos en los que, en realidad, no se documentan imágenes pornográficas sino que, por el contrario, se capturan o muestran escenas de abuso sexual infantil (ver Carla Delle Donne, "Imágenes de abuso sexual infantil: el art. 128 del Código Penal y el Convenio de Ciberdelincuencia de Budapest", *Revista de Derecho Penal y Procesal Penal*, Abeledo Perrot, marzo de 2017).

diata de los datos de tráfico definidos en el artículo 1.d del convenio como aquellos "datos que tienen relación con una comunicación por medio de un sistema informático" y producidos por el mismo sistema informático que permiten identificar la cadena de comunicación "indicando el origen, el destino, el itinerario, la hora, la fecha, el tamaño y la duración de la comunicación o el tipo de servicio subyacente" (artículo 17); c) las órdenes de presentación como medidas de prueba para el registro y el secuestro de datos que se encuentren en posesión de de terceras personas, por ejemplo, los proveedores de servicios de internet (ISP según sus siglas en inglés) que custodian datos de tráfico esenciales para una investigación penal (artículo 18); d) el registro y secuestro de los datos a los efectos de la obtención, preservación de la integralidad y copiado de la prueba informática que se encuentre en el territorio de los Estados parte (artículo 19); e) la obtención en tiempo real de datos de tráfico que implica la intervención de las comunicaciones electrónicas en el mismo momento en el que se producen para cualquier tipo de delito (artículo 20); f) interceptación de datos relativos al contenido únicamente para los delitos que cada Estado parte defina como "graves" que justificarían esa injerencia estatal en el ámbito de la privacidad, es decir, de todos los datos que no son datos de tráfico y que hacen a la comunicación en sí misma (artículo 21); g) reglas procesales sobre competencia que, al igual que otros tratados internacionales, otorga primacía al principio de territorialidad en primer lugar y, luego, dispone la aplicación del principio de nacionalidad activa para aquellos casos en los que el delito cometido se encuentre prohibido en el Estado en el que se cometió el delito o si el delito no cae bajo la jurisdicción territorial de ningún Estado (artículo 22.1). Las reglas sobre competencia también establecen el principio de *aut dedere aut iudicare* que exige que el Estado que deniegue la extradición de un presunto autor de alguno de los delitos previstos en el convenio, lo juzgue ante sus propios estrados (artículo 22.3); y no restringen la aplicación de otro modo de establecer la competencia en materia penal que los Estados tenga previsto en sus ordenamientos internos (artículo 22.4).

2.4.3. Cooperación internacional

En materia de lucha contra la delincuencia informática, la tipificación de los delitos enunciados en el convenio por parte de los Estados parte implica evitar lagunas del Derecho que fortalecen la lucha contra la ciberdelincuencia y tienden a erradicar la impunidad. Es por ese motivo que, en materia de Derecho sustantivo, la tipificación de las conductas delictivas es clave a los fines de la cooperación internacional, eventuales pedidos de extradición y a los fines de responder solicitudes de asistencia mutua en investigaciones iniciadas en otras jurisdicciones.

Es que si se considera el alcance global de la ciberdelincuencia, la falta de tipificación de esas conductas delictivas así como también la ausencia de normativa procesal que permita, por ejemplo, la recolección de evidencia digital para una investigación iniciada en Estados en cuyo territorio no se produjo el resultado lesivo, atentarían directamente contra los objetivos principales del convenio, en particular, contra las medidas sobre asistencia mutua, por ejemplo, de conservación rápida de datos informáticos almacenados, el acceso transfronterizo de datos informáticos y la obtención en tiempo real de datos relativos al tráfico.

En ese sentido, debe considerarse que uno de los mayores desafíos en materia de investigación de delitos informáticos se encuentra en la volatilidad de las pruebas informáticas. En efecto, la facilidad con la que se puede eliminar, dañar, perder o destruir la prueba digital plantea la necesidad de establecer mecanismos eficaces de cooperación internacional que no respondan a los cánones formales tradicionales. Es por ese motivo que, a los fines de la pronta recolección y conservación de la prueba electrónica, el informe explicativo del convenio indica que la cooperación internacional debe estar orientada a la circulación fluida y rápida de la información y las pruebas a nivel internacional.

Asimismo, en materia de cooperación internacional, el convenio es flexible e inclusivo de todo instrumento de cooperación en materia penal y legislación interna que puedan invocar los Estados parte que no sea el propio Convenio sobre Ciberdelito a los fines de cooperar en una investigación penal (artículo 23).

En materia de extradición, el artículo 24 del convenio dispone que todos los presuntos responsables de los delitos previstos en los artículos 2 a 11 podrán ser pasibles de extradición en la medida en que se cumpla el principio de doble incriminación que exige que la conducta sea punible tanto en el Estado requirente como en el Estado requerido y que el monto mínimo de la pena privativa de la libertad prevista para el delito que se impute, sea de un año. La decisión de fijar ese monto de pena privativa de la libertad se encuentra en consonancia con el artículo 2 del Convenio Europeo de Extradición.

Los principios generales relativos a la asistencia mutua están contemplados en los artículos 25 a 35 del convenio. Esas disposiciones tienden a flexibilizar las comunicaciones entre los Estados parte a los fines de cooperar de manera efectiva en la recolección y preservación de evidencia digital. También requieren de la adopción de medidas legislativa que no atenten en contra de la cooperación que exige que todos los Estados parte cuenten una legislación mínima que les permita alcanzar ese objetivo con éxito.

Por último, resulta relevante destacar que en relación con la efectiva interacción de las redes de cooperación, el artículo 35 del convenio dispone la creación de redes 24x7 que no solo faciliten los canales de extradición, sino que puedan asistir de manera inmediata en la conservación de datos, recolección de pruebas y que cuente, al mismo tiempo, con los conocimientos técnicos suficientes a los efectos de ofrecer consejos técnicos.

2.4.4. Reservas

El convenio prevé la posibilidad de hacer reservas en el artículo 42. La posibilidad de formular reservas forma parte de una enunciación taxativa ya que esa disposición establece que los Estados pueden realizar únicamente las reservas que se encuentran expresamente previstas en el convenio al firmar o depositar el instrumento de ratificación, aceptación, aprobación o adhesión.

La razón por la cual en el momento de la elaboración del texto se dispuso un régimen especial de reservas —que en materia de tratados pueden

únicamente realizarse en la medida en que no sea incompatible con el objeto y fin del instrumento internacional de que se trate, según lo dispone el artículo 19.c de la Convención de Viena sobre Derecho de los Tratados— se encuentra en el informe explicativo. Allí, en el párrafo 320, se indica que "las posibilidades de reserva tienen la finalidad de permitir que el mayor número posible de Estados lleguen a ser partes del convenio, al mismo tiempo que permiten a dichos Estados mantener ciertos enfoques y conceptos que sean coherentes con su legislación nacional".

De esa manera, el tratado fija un *numerus clausus* de reservas que asegura que los terceros Estados que quieran adherir no invoquen su legislación interna o tradición jurídica como motivo para no formar parte del régimen jurídico de Budapest, así como también mantiene el objeto principal del convenio.

En lo que a las reservas en especial se refiere, el artículo 4.2 dispone que los Estados parte puede hacer una reserva sobre la tipificación del delito contra la integridad de los datos o daño informático que cause un perjuicio grave. En ese supuesto, debe interpretarse que el convenio establece la facultad de los Estados parte de incorporar como elemento del tipo penal el grave perjuicio ocasionado por el daño. Sin embargo, si algún Estado decidiera hacer una reserva sobre este delito debería explicar al secretario general la interpretación de lo que constituye un perjuicio grave en la oportunidad de efectuar la reserva, tal como lo indica el informe explicativo.

El artículo 6.3 ofrece la posibilidad de efectuar una reserva sobre la incorporación del delito de abuso de dispositivos o datos de acceso para la comisión de alguno de los delitos previstos en los artículos 2 a 5 que protegen la confidencialidad, la integridad y la disponibilidad de los datos y los sistemas informáticos. La reserva no recae sobre todos los supuestos previstos en el artículo 6.1, sino que se encuentra sujeta a una condición: los Estados, al efectuar la reserva, pueden elegir no incorporar en su ordenamiento interno el delito de abuso de abuso de dispositivos en la medida en que no recaiga sobre el delito previsto en el artículo 6.a.ii. En consecuencia, a los fines de cumplir con el objeto y fin del tratado, los Estados deben cumplir con un estándar mínimo y deberán, necesariamente, tipificar en sus ordenamientos internos la venta,

distribución o puesta a disposición de una contraseña informático o un código de acceso.

El artículo 9.4 establece las reservas totales o parciales que pueden realizar los Estados relativas a los delitos informáticos que atentan contra la sexualidad de los menores de edad. Esa disposición autoriza a los Estados a no incorporar en su Derecho interno tipos penales que repriman la adquisición de material de abuso sexual infantil para uno mismo o para terceros y la tenencia simple de ese tipo de material que estuviere guardada en un sistema informático o sistema de almacenamiento informático. Asimismo, habilita a los Estados a que limiten el concepto de pornografía infantil —que debería denominarse material de abuso sexual infantil—[14] a los fines que solo comprenda a menores adoptando comportamientos sexualmente explícitos y no incluya ese tipo de material que involucre a personas adultas que aparentan ser menores de edad y las imágenes realistas de menores en las que no aparece un menor de edad real adoptando un comportamiento sexualmente explícito.

El artículo 10.3 establece la reserva para la tipificación de conductas que infrinjan los derechos de propiedad intelectual. La redacción de ese apartado parecería otorgar amplias facultades a los Estados para imponer penas para las violaciones a los derechos de autor, sin embargo, la reserva solo puede realizarse teniendo en cuenta las obligaciones asumidas con la ratificación de otros tratados internacionales que protegen la propiedad intelectual y en especial consideración del artículo 61 del acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio que establece un régimen penal para las infracciones contra los derechos de autor cuando tengan escala comercial.

El artículo 11.3 permite que los Estados no incluyan en sus legislaciones punición de la tentativa de los delitos previstos en el convenio. El objetivo de esa reserva, según surge del informe explicativo del convenio, es permitir que la mayor parte de los Estados ratifiquen el tratado.

El artículo 14.3 permite que los Estados formulen dos tipos de reservas sobre la recopilación en tiempo real de los datos de tráfico. La reserva prevista en el artículo 14.3.a permite que los Estados cuyas legislaciones

[14] Ibídem.

internas no posibiliten la recopilación de los datos de tráfico no se encuentre en la convención un obstáculo para formar parte del régimen de lucha contra la ciberdelincuencia. La reserva no puede recaer sobre más delitos que los delitos sobre los que se haga la misma reserva en el supuesto del artículo 21 en relación con la recopilación en tiempo real de los datos de tráfico. La reserva tiene carácter restrictivo y debería permitir de la manera más amplia el establecimiento de procedimientos para obtener en tiempo real datos relativos al tráfico. La reserva prevista en el artículo 14.3.b dispone la posibilidad para los Estados de no cumplir con la obligación de interceptar datos de tráfico y de contenido de comunicaciones entabladas en sistemas informáticos que se hayan puesto en funcionamiento para un grupo restringido de usuarios (artículo 14.3.b.i), cuando no se utilicen redes públicas de comunicación que a su vez no se encuentren conectadas a otros sistemas informáticos (artículo 14.3.b.ii).

El artículo 22 del convenio establece las reglas sobre jurisdicción y delimita los casos en los que los Estados parte podrán ejercer su competencia. Esos principios establecidos afirman el principio de territorialidad (artículo 22.1. a, b y c), el principio de nacionalidad activa (artículo 22.1.d), así como también reconocen la aplicación extraterritorial de la ley penal en dos casos: si el accionar constituye un delito en el lugar en el que se cometió o si ningún Estado tiene competencia territorial para perseguir y juzgar alguno de los delitos previstos en el convenio. Si bien es cierto que esas reglas son amplias, en consideración a los distintos sistemas jurídicos, en especial, el sistema jurídico continental o de tradición civilista, los redactares del convenio dispusieron la posibilidad de formular reservas sobre el artículo 22.1.b a 22.1.d (artículo 22.2). La posibilidad de efectuar esas reservas obliga a los Estados a aplicar siempre el principio de territorialidad entendido en un sentido estricto de espacio territorial y no por extensión, es decir, que los Estados podrían no aplicar la ley penal teniendo en cuenta la ley del pabellón de buques y aeronaves. Así como también exige que los Estados cumplan con el principio de extraditar a juzgar —*aut dedere aut iudicare*— por cualquiera de los delitos previstos en el convenio (artículos 22.3 y 24).

El artículo 29.4, relativo a la conversación rápida de datos informáticos almacenados, permite que los Estados formulen reservas a la

obligación de cumplir con cualquier solicitud de asistencia mutua para la preservación de prueba digital por delitos cometidos en el extranjero que no se encuentren tipificados en el ordenamiento interno. Esa reserva permite que los Estados exijan el cumplimiento del principio de doble incriminación aun en materia procesal para la conservación de prueba digital. La reserva, entonces, establece una excepción al principio general establecido en el convenio y los Estados que efectúen esa reserva tendrán la posibilidad de denegar cualquier solicitud de asistencia mutua para la conservación de datos informáticos fundada en la falta de cumplimiento del requisito de doble tipificación.

Por último, la reserva prevista en el artículo 41 sobre la obligación de adecuar la normativa interna de los Estados contratantes resulta aplicable para aquellos Estados federales cuyos Estados, departamentos o provincias conservan, entre otras, la potestad de dictar su propia legislación penal y procesal penal[15]. El límite que establece esa reserva de términos amplios y poco claros es que los Estados no podrían invocar esa reserva para incumplir con cualquier pedido de cooperación o asistencia mutua.

2.5. La ratificación del Convenio sobre Ciberdelito en la República Argentina

2.5.1. La sanción de la Ley N.º 27.411

El Convenio sobre Ciberdelito del Consejo de Europa se incorporó al Derecho interno a través de la Ley N.º 27.411 (en adelante, "la ley"). La ley fue sancionada el 21 de noviembre de 2017, promulgada por el decreto N.º 1.039/2017 el 14 de diciembre de 2017 y publicada un día después en el Boletín Oficial.

La ley cristaliza el largo proceso de adhesión que nuestro país iniciara durante la Octupus Interface Conference de Cooperación contra la Ciberdelincuencia llevada a cabo en la sede del Consejo de Europa en Estrasburgo, Francia, entre el 23 y 25 de marzo de 2010. Durante

[15] Tal es el caso de los Estados Unidos, uno de los Estados invitados por el Consejo de Europa para participar de las negociaciones y elaboración del convenio.

esa conferencia, los integrantes de la delegación que representaban a la República Argentina presentaron la solicitud formal de invitación de adhesión al convenio a los efectos de iniciar el trámite de adhesión previsto para los Estados que no forman parte del Consejo de Europa y que no participaron en su elaboración de acuerdo con lo estipulado en el artículo 37 del convenio. La invitación a adherir al convenio fue extendida por el Consejo de Europa el 20 de septiembre de 2010 y con junto con ella quedó habilitada la vía parlamentaria que concluyó siete años más tarde con la sanción de la Ley N.º 27.411.

La promulgación de la ley permitió que, a través del Ministerio de Relaciones Exteriores y Culto, el 5 de junio de 2018 se depositara el instrumento de adhesión ante el secretario general del Consejo de Europa. En consecuencia, el convenio entrará en vigencia el 1 de octubre de 2018, es decir, transcurridos los tres meses contados a partir de la fecha del depósito (artículo 37.2).

La ratificación del convenio representa un paso significativo para nuestro país frente a la comunidad internacional. Y si bien es cierto que ser Estado parte del régimen de lucha contra la ciberdelincuencia nos presenta ante nuevas obligaciones que exigirán la armonización normativa para conciliar nuestra legislación con las disposiciones del instrumento internacional, no menos cierto es que también nos permitirá capitalizar la experiencia de larga data del Consejo de Europa en materia de prevención, persecución y juzgamiento de delitos informáticos y recurrir a los canales de cooperación y asistencia mutua para interactuar con otros Estados parte.

2.5.2. Las reservas dispuestas en la Ley N.º 27.411

La ley que incorporó a nuestro ordenamiento interno el convenio dispuso algunas de las reservas que, de manera expresa, autoriza el artículo 42. Así, pues, el artículo 2 de la ley dispone que al efectuarse el depósito del instrumento de adhesión deben realizarse las reservas que se describen a continuación.

El artículo 2.a establece que no será obligatorio para nuestro país la incorporación del delito de tenencia simple de dispositivos, palabras de acceso o datos informáticos que permitan la comisión de los delitos

previstos en los delitos 2 a 5 contra la confidencialidad, la integridad y disponibilidad de los datos y sistemas informáticos. El motivo que fundamentó la reserva estriba en que ese delito tipificaría un acto preparatorio que sería ajeno a la tradición legislativa en materia jurídico penal.

Los motivos que justifican la reserva no se ajustan exactamente al real fundamento que podría habérsele otorgado. Es que si bien es cierto que en torno a los delitos de tenencia existe en nuestro país, tanto en la doctrina como en la jurisprudencia, un debate que busca el equilibro entre el ejercicio del poder estatal y el principio de reserva previsto en el artículo 19 de la CN, no menos cierto es que hay conductas que, por razones de política criminal, el legislador decidió elevar a la categoría de tipo penales[16]. Así, pues, podría haberse eximido de la obligación internacional de tipificar la tenencia de dispositivos necesarios para la comisión de los delitos previstos en los artículos 2 a 5 del convenio, invocando otras razones —que exceden el análisis que aquí propongo—, porque nuestro ordenamiento sustantivo criminaliza delitos peligro, que como tales conllevan un adelantamiento de la punición pero que constituyen una herramienta única para proteger bienes jurídicos de gran trascendencia.

Los artículos 2.b y 2.c establecieron una serie de reservas relativas al artículo 9 del convenio que insta a los Estados a tipificar las conductas relacionadas con el material de abuso sexual de menores[17] online. Las reservas se ajustan a la redacción del artículo 128 del CP según la modificación introducida por la Ley N.º 26.388, es decir, la redacción vigente a la fecha de la sanción de la ley. Esa aclaración es necesaria porque la descripción de los tipos penales previstos en el artículo 128 del CP fueron modificados cuatro meses después de la promulgación de la ley con la sanción de la ley 27.436[18].

Esa última modificación legislativa al incorporar al ordenamiento sustantivo la tenencia dolosa de "toda representación de un menor de

[16] Por ejemplo, la tenencia ilegítima de armas (artículo 189 bis del CP) y el acoso sexual online de menores (artículo 131 del CP).

[17] El artículo 9 tipifica las conductas relacionadas con lo que denomina pornografía sexual infantil. Sin embargo, me refiero a imágenes de abuso sexual infantil en lugar de utilizar la expresión de pornografía infantil a los fines de ajustar la terminología que corresponde utilizar en los casos de abusos sexuales de menores en los que las relaciones sexuales, tal como se señaló en la nota 12.

[18] La Ley N.º 27.436 fue sancionada el 21 de marzo de 2018 y publicada en el Boletín Oficial el 23 de abril de 2018.

18 años dedicado a actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales", dejó sin efecto la reserva prevista en el artículo 2.c de la ley que la Argentina había efectuado con relación a la obligación de tipificar la tenencia simple de imágenes de abuso sexual infantil. Esa reserva señalaba que la tenencia, de acuerdo con nuestra legislación, estaba reprimida únicamente cuando se podían acreditar los fines de comercialización o distribución como ultraintención o elemento subjetivo del tipo distinto del dolo.

La reserva que sigue vigente en relación con la protección online de la integridad sexual de los menores de edad, es la que contempla el artículo 2.b, que excluye la obligación de incorporar al ordenamiento interno: a) la adquisición para uno mismo o para terceros[19] de material de abuso sexual infantil a través de un sistema informático, y b) la ampliación de la definición de "toda representación" que —como elemento normativo del tipo penal— no comprenderá ni las imágenes que incluyan únicamente a personas que parezcan menores de edad sin serlo, ni las imágenes realistas[20].

Los legisladores invocaron razones de incompatibilidad con el CP vigente conforme a la reforma introducida por la Ley N.º 26.388 que modificó por primera vez ese cuerpo normativo para incorporar delitos informáticos. Sin embargo, lo cierto es que la adquisición de material de abuso sexual infantil se encuentra reprimida en el artículo 128 del CP en el verbo típico de comerciar que castiga tanto al que compra como el que vende. El problema se plantea si se entiende que la traducción que corresponde darle al verbo "*procure*" de la versión oficial en inglés del convenio, es la de buscar que, tal como expresa el informe explicativo del convenio, se refiere a la obtención activa de material de abuso sexual infantil, por ejemplo, descargándola porque esa conducta no es incompatible con el código vigente sino que es atípica[21]. En ese mismo sentido,

[19] La traducción oficial del Convenio de Budapest aprobada eligió la expresión *"procuring… for oneself or for other person"* como "procurarse o de procurar para otro". Sin embargo, considero que la traducción que más se ajusta a los términos del convenio es aquella que sugiere que los Estados parte deben tipificar la conducta de adquirir.

[20] Las imágenes realistas en los términos del convenio son las imágenes que no comprenden a un niño real sometido a una situación de abuso sexual. En esa categoría se pueden incluir, por ejemplo, las imágenes digitalmente manipuladas, las generadas únicamente por medios digitales tales como las animaciones.

[21] Para un estudio de las conductas reprimidas en el artículo 128 del CP, ver Carla Delle Donne,

cabe señalar que la necesidad de excluir de la definición de "toda representación" las imágenes en las que incluyen personas adultas que parezcan menores o las imágenes realistas, tampoco resultaría incompatible con el CP vigente. Es que el legislador perdió de vista que lo que hizo al realizar esa reserva fue coartar las facultades interpretativas del juez —y de las partes del proceso— al restringir la interpretación de cuáles son las imágenes que comprende "toda representación" como objeto del delito y elemento normativo del tipo penal previsto en el artículo 128 del CP.

En relación con las normas del convenio relativas a la jurisdicción, la República Argentina hizo una de las reservas previstas en el artículo 22.2 del convenio y dispuso en el artículo 2.d de la ley que no será aplicable en nuestro país la obligación prevista en el artículo 22.1.d, que establece la aplicación extraterritorial de la ley penal para delitos cometidos por sus nacionales si el delito es susceptible de sanción penal en el lugar en el que se cometió o si ningún Estado tiene competencia territorial para perseguirlo penalmente. La reserva es un acierto del legislador, puesto que recepta las reglas establecidas en el artículo 1 del CP. Sin embargo, considero que la ratificación del convenio era una buena posibilidad para no hacer esa reserva y, de ese modo, habilitar la vía parlamentaria para promover una nueva modificación del ordenamiento sustantivo que amplíe la reforma introducida por el artículo 29 de la Ley N.º 27.401 promulgada el 1 de diciembre de 2017 que incorporó al artículo 1 del CP la posibilidad de que los jueces argentinos puedan ejercer su competencia por el delito de cohecho activo de funcionarios público extranjeros o de organismos internacionales previsto en el artículo 258 bis del CP cuando fuere cometido por ciudadanos argentinos en el extranjero (principio de nacionalidad activa).

Por último, la ley hace reserva del artículo 29.4 del convenio porque "el requisito de la doble incriminación es una de las bases fundamentales de la Ley de Cooperación Internacional en Materia Penal N.º 24.767"; y como principio esencial en materia de extradición y asistencia legal mutua, la reserva —que no altera el objeto del convenio— resulta ajustada a la normativa interna y vigente en nuestro país.

"Imágenes de abuso sexual infantil: el art. 128 del Código Penal y el Convenio de Ciberdelincuencia de Budapest", *Revista de Derecho Penal y Procesal Penal*, Abeledo Perrot, marzo de 2017.

2.5.3. La adecuación normativa interna a los estándares del convenio previa a la ratificación

El proceso de armonización del ordenamiento interno argentino comenzó mucho tiempo antes de la ratificación del convenio. En efecto, uno de los recaudos que adoptó nuestro país antes de ser invitado a adherir al régimen jurídico de lucha contra la ciberdelincuencia fue la primera modificación del CP, el 4 de junio de 2008, con la sanción de la Ley N.º 26.388, publicada en el Boletín Oficial el 25 de junio de 2008. Esta ley constituyó el primer eslabón del proceso de conciliación progresiva de la legislación argentina con el convenio, ya que incorporó los primeros delitos informáticos[22].

La Ley N.º 26.388 incorporó al ordenamiento sustantivo la mayoría de las conductas previstas en el convenio que no se encontraban de ningún modo previstas en el ordenamiento sustantivo. Esa modificación, entre otros motivos que exceden el objeto del presente trabajo, se incorporó para demostrar que la República Argentina se encontraba en condiciones de asumir las obligaciones internacionales que conllevaba presentar ante el Comité del Consejo de Europa la solicitud de invitación a adherir al convenio.

En cuanto aquí interesa, la Ley N.º 26.388: a) modificó la redacción del artículo 128 del CP para incorporar un amplio catálogo de conductas típicas que reprimen toda la cadena de producción y distribución de imágenes de abuso sexual infantil e incluyó los medios informáticos como medio de comisión del delito; b) alteró el título del capítulo III

[22] A los fines de definir el concepto de delitos informáticos, se pueden considerar dos categorías: los delitos netamente informáticos o propios que constituyen todas las acciones típicas que, cometidas mediante el uso de un dispositivo informático, recaen sobre los sistemas informáticos, es decir, hechos ilícitos que afectan: a) la operatividad y el normal funcionamiento de un sistema informático; y b) las comunicaciones electrónicas o digitales y los datos informáticos que atentan contra la integridad, confidencialidad y disponibilidad de esas comunicaciones o datos informáticos; y los delitos informáticos impropios son delitos informáticos en un sentido más genérico porque el accionar disvalioso se consuma a través de un dispositivo electrónico conectado a Internet que, en definitiva, involucra la utilización de un medio informático para fines delictivos. En esta categoría se incluyen aquellas conductas típicas que preveía el código penal antes de la incorporación de la Ley N.º 26.388 y que requieren técnicas poco sofisticadas.

ampliando el bien jurídico protegido ya no solo a la confidencialidad de los secretos sino también a la privacidad y, en esa línea, modificó la redacción de los artículos 153, 155, 157 y 157 bis e incorporó el artículo 153 bis para castigar conductas que atenten contra la confidencialidad, integridad y normal funcionamiento de las comunicaciones informáticas, los sistemas informáticos, las bases de datos informáticos y los datos informáticos; c) incorporó el inciso 16 al artículo 173 para crear la estafa informática como aquella conducta que se perpetra a través de cualquier manipulación informática; d) tipificó el daño informático en el artículo 183 y el daño agravado en el artículo 184 incisos 5 y 6.

El puntapié dado por la Ley N.º 26.388 lo continuó la Ley N.º 26.904 publicada en el Boletín Oficial el 11 de diciembre de 2013. Esa nueva ley incorporó el acoso online de menores (denominado también *grooming*)[23].

2.5.4. Las reformas legislativas pendientes tras la ratificación del convenio

La sanción de las leyes N.º 26.388 (2008) y N.º 26.904 (2013) fueron hitos fundamentales en términos de adecuación normativa de la legislación argentina al convenio y a la realidad criminológica actual. Las modificaciones incorporadas por esas leyes resultan eliminaron lagunas normativas que existían y que forzaron interpretaciones que eliminaron lagunas normativas.

Asimismo, tal como se expresara en el apartado relativo a las reservas efectuadas al sancionar la ley que ratifica el convenio, una nueva modificación del Código Penal cerró aún más la brecha de impunidad para los delitos cometidos contra menores de edad por medios informáticos con la sanción de la Ley N.º 27.436 (2018) que amplía las conductas típicas previstas en el artículo 128 del CP y se adecua a los estándares fijados por el convenio.

[23] Para un estudio del tema, ver Carla Delle Donne, "El delito informático de *grooming* y la necesidad de la reforma del Código Penal", *Revista de Derecho Penal y Procesal Penal*, Abeledo Perrot, mayo de 2012; y Carla Delle Donne y Pablo Palazzi, "Delincuencia online que afecta menores: el *grooming* tipificado como corrupción de menores agravada", *Revista de Derecho Penal y Procesal Penal*, Abeledo Perrot, enero de 2014.

Sin embargo, existen todavía deudas pendientes en materia legislativa para armonizar el CP y el Código Procesal Penal de la Nación (CPPN) a las obligaciones asumidas al ratificar el convenio.

En materia de Derecho penal sustantivo, sería necesaria la modificación de la Ley N.º 11.723 que protege la propiedad intelectual a los fines de actualizarla mediante la incorporación de nuevos delitos y redefinición de los existentes. Recordemos que, en lo que a los derechos de propiedad intelectual se refiere, la Ley N.º 11.723 fue promulgada en 1933 y que la Ley N.º 23.741 que incorpora el tipo penal previsto en el artículo 72 bis data del año 1989; mucho tiempo antes de que se pudieran prever los adelantos tecnológicos que trajeron aparejadas nuevas conductas evidentemente delictivas, de particulares características, nuevos modos de comisión y perpetrados en Internet a través de sistemas informáticos como medio comisivo.

Por otra parte, cabe preguntarse si el delito de daño tal como se encuentra tipificado alcanzará posibles atentados contra las infraestructuras típicas o si el sabotaje previsto en la Ley N.º 13.985 de 1950 será suficiente para perseguir posibles ciberataques.

La reforma legislativa introducida por la Ley N.º 26.388 no previó la modificación del artículo 73 inciso 2 del CP en cuanto exige que los delitos de violación de secretos, salvo en los casos de los artículos 154 y 157, son de acción privada, pero que, no obstante ello, deberían ser considerados delitos de acción pública.

En lo que se refiere a las normas procesales, el CPPN aprobado por la Ley N.º 27.063, cuya vigencia fue aplazada, incluye la incautación de datos informáticos a través del registro de un sistema informático, la interceptación de comunicaciones electrónicas. Más avanzados se encuentran en materia legislativa los códigos procesales penales provinciales, por ejemplo, el de Neuquén, que disponen tanto el secuestro de información digital como el acceso remoto como técnica de investigación.

A nivel federal y nacional, el Código Procesal vigente no dispone ninguna norma relativa al secuestro de prueba digital (datos de tráfico, datos de contenido y prueba digital en general) como medio probatorio, así como tampoco prevé la intervención de comunicaciones electrónicas ni el acceso remoto como medio probatorio. En la actualidad, las inves-

tigaciones se fundamentan —de manera tácita— en el artículo 206 del CPPN que admite la libertad probatoria con el objetivo de descubrir la verdad real[24].

Otra cuestión será analizar la posibilidad de incluir como posibles agentes encubiertos o agentes reveladores, en los términos previstos en la Ley N.º 27.319, a ciberpolicías y la posibilidad de realizar tareas de prevención policial online o ciberpatrullaje.

3. Conclusiones

Cuando un Estado presta su consentimiento en obligarse por los términos de un tratado internacional, genera la obligación de armonizar su Derecho interno con las disposiciones del instrumento internacional. Esas obligaciones internacionales nacieron para nuestro país el 5 de junio de 2018 con el depósito del instrumento de adhesión ante el secretario general del Consejo de Europa.

De la mano de ese compromiso surge la necesidad de adecuar la legislación interna a los términos del convenio para ampliar el catálogo de los tipos penales ya incorporados al CP e introducir las reformas procesales que respondan a los estándares internacionales.

La reforma legislativa es necesaria para cumplir con las obligaciones internacionales pero no será suficiente. La investigación y persecución de los delitos informáticos exige, asimismo, la creación de instituciones especializadas y la capacitación de los operadores de judiciales y de las fuerzas de seguridad para alcanzar una mejor y más cabal comprensión de la ciberdelincuencia en todos sus aspectos legales.

La respuesta a la lucha contra la ciberdelincuencia requiere procedimientos que brinden respuestas rápidas y novedosas para nuestra cultura forense. Por esa razón la intervención proactiva del sector privado, tal como lo prescribe el convenio con la obligación de presentar las órdenes de presentación ante la justicia que se requieran, será una arista sobre la que trabajar con ahínco. En ese mismo sentido, la cooperación in-

[24] El riesgo que representan las lagunas normativas en materia de Derecho procesal penal es que en muchos casos se aplican por analogía normas vigentes (artículo 2 *in fine* CPPN).

ternacional y la asistencia mutua, como otra de las claves del convenio, requerirán la respuesta inmediata que no atente con la preservación de la prueba y exigirá, de ese modo, mecanismos fluidos que acorten los tiempos habituales que demanda el trámite de los exhortos en el plano internacional.

Los desafíos de formar parte del Convenio sobre Ciberdelito de Budapest son innumerables. Sin embargo, las ventajas que representa haberlo ratificado los justifican porque abren el camino que nos permitirá crecer en materia de lucha contra la ciberdelincuencia.

Derecho de supresión y libertad de expresión en el marco de redes sociales

por Lucía Suyai Mendiberri

Resumen: El presente trabajo tiene por objeto analizar la procedencia del derecho de cancelación en el marco de contenidos publicados en redes sociales por terceros que afecten la intimidad del individuo. Adicionalmente, se analizará la competencia de la Agencia de Acceso a la Información Pública para resolver estos conflictos.

Voces: derecho de cancelación, derecho de supresión, redes sociales, hábeas data, derecho a la intimidad, derecho a la intimidad en Internet, derecho a la privacidad, autodeterminación informativa, redes sociales, libertad de expresión, Ley de Protección de Datos Personales, competencia de la Agencia de Acceso a la Información Pública.

Abstract: This paper aim to analyse the cancellation right regarding third parties posts on social networks which constitute privacy right infringements. Also, it will be under the scope of analysis the competence of the Access to Public Information Agency to resolve these conflicts.

Key words: cancellation right, social networks, habeas data, privacy right, privacy right on Internet, information self-determination, freedom of speech, personal data protection law, Access to Public Information Agency competence.

1. Introducción

La aparición de Internet, su masividad y el avenimiento de nuevos jugadores en su ecosistema que procesan millones de datos por segundo, como son los buscadores y las redes sociales, vienen desafiando hace ya algunos años los paradigmas relacionados con el derecho a la intimidad y la libertad de expresión. La explosión de Internet y de las redes sociales significó un impacto aún mayor que la intromisión de la televisión en el

seno de las familias, dado que se entrelazó en la vida de los individuos a tal punto que preformó su comportamiento y perforó los espacios tradicionalmente reservados a la intimidad[1].

El comportamiento de los sujetos en las redes sociales, que se centra básicamente en compartir y exhibir su identidad, intimidad y su subjetividad, disputa la concepción de los aspectos tradicionalmente protegidos por el derecho a la intimidad y las herramientas que poseemos para protegerlo. En tal sentido, parece inminente un proceso de *des-construcción* de aquello que entendemos protegido por el derecho a la intimidad. Asimismo, siempre que Internet, en general, y las redes sociales en particular presupongan una particular dinámica dentro de la cual un individuo exhibe y comparte su información en un ecosistema cuyo flujo hace difícil establecer medidas efectivas para controlar la diseminación de tal información, resulta pertinente revisar las herramientas jurídicas que los individuos detentan para defenderse y proteger su intimidad.

Ante el particular desafío que representa la dinámica antes expuesta, las leyes de protección de datos y la autodeterminación informativa del individuo han cobrado especial atención en el último tiempo.

En línea con lo anterior, este trabajo se propone analizar la Ley N.º 25.326 en relación con la protección de Datos Personales Argentina como herramienta de salvaguarda del derecho a la intimidad de los individuos en el marco de las redes sociales. En particular, se centrará en la procedencia del derecho de cancelación o supresión previsto en tal normativa ante contenidos publicados en redes sociales que afecten la intimidad del individuo, teniendo en consideración la tensión evidente con la libertad de expresión. Por último, reservaré un capítulo para el análisis de la competencia de la Agencia de Acceso a la Información Pública en su calidad de Autoridad de Control de la Ley de Protección de Datos Personales para decidir con relación al derecho de cancelación en el marco de redes sociales.

[1] Resulta ilustrativa la omnipotencia de Internet en la cotidianidad si pensamos en el tiempo que pasamos con nuestro *smartphone*, navegando en diferentes redes sociales, o en la facilidad con la que hacemos públicas imágenes de tal cotidianidad con nuestras familias o amistades a través de las redes sociales.

2. La autodeterminación informativa como derecho constitucional

La autodeterminación informativa se define por primera vez en una sentencia del Tribunal Constitucional Federal Alemán dictada el 15 de diciembre de 1983. En aquel antecedente se explica que dicha facultad se relaciona con "[…] el libre desarrollo de la personalidad [que] presupone en las modernas condiciones para el procesamiento de datos, la protección de los individuos frente a la ilimitada recolección, archivo, empleo y retransmisión de sus datos personales. […] El derecho fundamental garantiza de esta manera la capacidad del individuo principalmente para determinar la transmisión y empleo de sus datos personales".[2]

El referido concepto cobró especial relevancia en los últimos tiempos, en los que la tecnología posibilitó el procesamiento masivo de datos e Internet y las redes sociales desafían los paradigmas ya constituidos relacionados con la intimidad y la capacidad del individuo de controlar la información en la red. En la actualidad, la identidad se construye y *desconstruye* a través de la extensa cantidad de información contenida en bases de datos, la que circula en Internet y en las redes sociales. Ante ese contexto, el derecho a la autodeterminación informativa no es más que la derivación necesaria del derecho a la intimidad en la era de la información, sirviendo no solo para repeler intromisiones indebidas a las esferas íntimas del individuo sino garantizándole al individuo su derecho de construir su identidad social y elegir cómo, dónde y hasta qué punto darse a conocer a terceros. En tal sentido se expresa también Alejandra Gils Carbó al concluir que este derecho "[…] está vinculado en forma inescindible al concepto de libertad y de dignidad de la persona humana".[3]

Osvaldo Alfredo Gozaíni[4] encuadra la "autodeterminación informa-

---

[2] Schwabe, Jürgen, Jurisprudencia del Tribunal Constitucional Federal Alemán, extractos de las sentencias más relevantes, Konrad-Adenauer-Stiftung Berlín, capítulo 7: sentencia BVerfGE 65. p. 95 [https://bit.ly/1kq1yPu].

[3] Gils Carbó, Alejandra M., "Régimen legal de las bases de datos y el hábeas data", *LL*, Buenos Aires, 2001, p. 16.

[4] El autor cita la definición de Herrán Ortiz, que dicta que "[…] el derecho a la autodeterminación informativa se construye tomando como fundamento el concepto de intimidad o vida privada, puesto que trata de ofrecer tutela a la persona respecto a sus datos de carácter personal, una posible utilización abusiva de los mismos mediante la informática y otro tratamiento automatizado. Ahora bien que nadie se confunda, mediante el derecho a la autodeterminación informativa no

tiva" dentro del hábeas data contenido en el párrafo tercero del artículo 43: "Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquéllos. No podrá afectarse el secreto de las fuentes de información periodística".

Víctor Bazán señala que el hábeas data reconoce el derecho de los individuos de controlar la transmisión y el uso de sus datos personales invistiendo embistiéndolo a tal individuo de los derechos de acceso, rectificación y cancelación.[5] En igual sentido se pronuncia Pablo Lucas Murillo de la Cueva al prescribir que, en razón de ser un bien jurídico tutelado por el hábeas data, esta acción se refiere a "preservar la información individual —íntima y no íntima— frente a su utilización incontrolada, arrancando, precisamente, donde termina el entendimiento convencional del derecho a la vida privada"[6].

La autodeterminación informativa como derecho incorporado por el artículo 43 con relación al hábeas data fue reconocido también por nuestra Corte Suprema de Justicia en el fallo "Suárez Mason, Carlos Guillermo s/ homicidio, privación ilegal de la libertad, etc."[7]. En dicho antecedente el juez Boggiano sostuvo que se había "[…] incorporado un nuevo derecho a la protección de los datos personales frente a cualquier intromisión arbitraria o abusiva que pudiera implicar una violación a la intimidad y a los demás derechos constitucionales. Pues tal derecho halla íntima relación con el derecho a la integridad, a la dignidad humana, a la identidad, al

se salvaguardan tan solo los datos que se denominan sensibles, sino que también aquellos que sin pertenecer a la esfera más próxima al individuo son susceptibles de daños a su imagen o al ejercicio pleno de sus derechos". Gozaíni, Osvaldo, "Derecho procesal constitucional. Hábeas data. Protección de daos personales, *Doctrina y jurisprudencia*, segunda edición ampliada y reformada, Santa Fe, Rubinzal Culzoni, 2011, p. 119.

[5] Bazán, Víctor, *El hábeas data y el derecho de autodeterminación informativa en perspectiva de derecho comparado*, p. 111.

[6] Murillo de la Cueva, Lucas Pablo, *El derecho a la autodeterminación informativa*, Madrid, Tecnos, 1990, p. 120, citado por Bazán, *El hábeas data y el derecho a la autodeterminación informativa en perspectiva de derecho comparado*, ob. cit., p. 114.

[7] CSJN, "Suárez Mason, Carlos Guillermo s/ homicidio, privación ilegal de la libertad, etc.", 13/8/1998 (Fallos: 321: 2031).

honor, a la propia imagen, a la seguridad, al de peticionar, a la igualdad, a la libertad de conciencia, a la libertad de expresión, de reunión, de asociación, de comerciar y con cualquier otro que, de uno u otro modo, pudiera resultar afectado".[8] En el mismo sentido se expidió el ministro de la Corte Fayt en "Ganora, Mario Fernando y otra s/ hábeas corpus".[9]

3. La aplicación de la Ley de Protección de Datos Personales y las plataformas de redes sociales

En vistas del desarrollo anterior, la autodeterminación informativa resulta el bien jurídico protegido en nuestra Ley de Protección de Datos Personales que reglamenta el hábeas data. El primer artículo de dicha ley sostiene: "La presente ley tiene por objeto la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean estos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre, de conformidad a lo establecido en el artículo 43, párrafo tercero de la Constitución Nacional". Con relación a esta definición, resulta necesario aclarar, por un lado, el alcance de la definición del "dato personal" y, por otro, los sujetos pasivos en cuanto a la expresión "privados a dar informes".

---

[8] Ibíd. voto del juez Boggiano.

[9] CSJN, "Ganora, Mario Fernando y otra s/ hábeas corpus", 16/09/1999 (Fallos: 322: 2139). Voto Carlos S. Fayt. Considerando 8.º: "[…] la protección legal que establece el hábeas data se dirige a que el particular interesado tenga la posibilidad de controlar la veracidad de la información y el uso que de ella se haga. En tal sentido, este derecho forma parte de la vida privada y se trata, como el honor y la propia imagen, de uno de los bienes que integran la personalidad. El señorío del hombre sobre sí se extiende a los datos sobre sus hábitos y costumbres, su sistema de valores y de creencias, su patrimonio, sus relaciones familiares, económicas y sociales, respecto de todo lo cual tiene derecho a la autodeterminación informativa. […] Se trata, pues, de una dimensión del derecho a la intimidad, en conexión de sentido con el art. 19 de la Constitución Nacional; constituye la acción que garantiza el derecho que toda persona tiene 'a decidir por sí misma en qué medida compartirá con los demás sus sentimientos, pensamiento y los hechos de su vida personal' (caso 'Ponzetti de Balbín', Fallos: 306: 1892). Por consiguiente, el hábeas data en tanto garantía de un derecho individual, personalísimo, solo puede ser ejercida por el titular del derecho a interponer la acción en defensa de aspectos de su personalidad vinculados con su intimidad que no pueden encontrarse a disposición del público ni ser utilizados sin derecho".

En cuanto al dato personal, la ley lo define como "información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables". En tal sentido explica Gozaíni que la ley "se refiere a cualquier tipo de información que un archivo tenga sobre una persona física o jurídica"[10]. La flexibilidad de la definición obedece a la naturaleza del bien jurídico protegido, toda vez que la autodeterminación informativa refiere a aquellos datos que se correspondan al ámbito de la intimidad del individuo los que pueden obedecer a la naturaleza de lo más variada.

La discusión doctrinaria en cuanto a los sujetos obligados delimitados por la frase "privados destinados a dar informes" quedó zanjada, y es unánime la interpretación actual en cuanto a que se *considera incluida cualquier base que contenga datos personales*. En virtud de lo expuesto, se ha sostenido reiteradamente que "la Ley resulta aplicable a todos los archivos y bases de datos privadas que no sean de uso personal; y entienden que deja de serlo cuando esos datos sirven para hacer evaluaciones que inciden en el goce o protección de los derechos del titular de los datos, es decir, que el uso de esos datos repercute en los derechos de una persona de manera relevante".[11] La misma interpretación ha sido sostenida por la Dirección Nacional de Protección de Datos Personales al entender que *cualquier base o archivo de datos que supere el uso estrictamente interno o personal de una persona* (como por ejemplo, una agenda de teléfonos personal), *encuadraría dentro de los casos comprendidos por la Ley de Protección de Datos Personales*[12]. En vistas de lo anterior, y siempre que las plataformas de redes sociales realicen un tratamiento de datos personales enmarcado en la norma, puede concluirse que la redacción antes reproducida no obsta a su aplicación a tales plataformas.

El proyecto de Ley de Protección de Datos Personales enviado recientemente al Congreso por el Poder Ejecutivo[13] supera definitivamente

[10] Gozaíni, Osvaldo, *Habeas Data (Ley 25.326 y reglamentación). Derecho Procesal Constitucional*, Santa Fe, Rubinzal Culzoni, 2002, p. 40.

[11] Palazzi, Pablo A., *La protección de los datos personales en la Argentina*, Errepar, 2004.

[12] En este sentido se ha pronunciado la Dirección de Protección de Datos Personales en la nota DNPDP N.º 816/2009-3471.

[13] Presentado por el Poder Ejecutivo a través del Mensaje MEN-2018-147-APN-PTE. Referencia: EX-2017-01309839-APN-DNPDP#MJ - Mensaje Ley de Protección de Datos

la discusión doctrinaria referida en el párrafo anterior, estableciendo su aplicabilidad siempre que *(i)* el responsable del tratamiento automatizado se encuentre en territorio nacional; *(ii)* el responsable se encuentre en un lugar donde se aplica la legislación nacional en virtud del Derecho Internacional o *(iii)* el tratamiento de datos personales refiera a titulares que residan en la Argentina y las actividades de tratamiento se encuentren relacionadas con ofertas e bienes o servicios, o con seguimientos de sus actos, comportamientos o intereses. Adicionalmente, define "tratamiento" como "[…] cualquier operación o procedimiento organizado, electrónico o no, que permita la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo o destrucción y, en general, el procesamiento de datos personales, así como también su cesión a través de comunicaciones, consultas, interconexiones o transferencias".[14]

4. El derecho de supresión

La autodeterminación informativa se refiere en definitiva a la soberanía del titular de los datos sobre los datos a ese referido. Tal soberanía presupone necesariamente garantizar el consentimiento del titular del dato y la posibilidad de ejercer su derecho de acceso, rectificación y supresión.

El derecho a la cancelación o supresión se encuentra regulado en el artículo 16 de la Ley de Protección de datos personales y en la misma Constitución Nacional, que establece que procede en casos de falsedad o discriminación. En consecuencia, y preliminarmente, se podría concluir que el derecho a suprimir el dato puede fundamentarse en diferentes supuestos: *(i)* revocación del consentimiento del titular de aquellos datos (toda vez que es condición necesaria para el tratamiento legítimo de

Personales [https://bit.ly/2Rhftvs]. El texto del anteproyecto ha sido originalmente redactado por la Autoridad de Control de la Ley de Protección de Datos Personales quien lo sometió a la deliberación de múltiples partes interesadas a través del programa Justicia 2020 del Ministerio de Justicia y Derechos Humanos. El texto ha sido modificado a partir de la introducción de aportes y comentarios de los sectores interesados siendo el texto enviado la segunda y última versión consolidada a través de tal programa deliberativo.

[14] Ibíd. artículo 2 del Proyecto de Protección de Datos Personales.

datos personales, si bien acepta rigurosas excepciones), *(ii)* inexactitud o falsedad el dato, y *(iii)* ante supuestos de discriminación. No obstante, entender que los fundamentos que habilitarían el mismo se agotan en tal enumeración llevaría a una interpretación abusiva, siempre que la misma Ley de Protección de Datos Personales entiende su objeto como la protección de datos "para garantizar el derecho al honor y a la intimidad de las personas".[15]

La flexibilización interpretativa propuesta en el párrafo anterior es también compartida por Gils Carbó, quien al analizar el texto constitucional del hábeas data sostiene que resulta claro que "[…] el texto constitucional no puede ser interpretado con el rigor de atribuirle una descripción tipificante o considerado con estrictez literal la mención de 'falsedad o discriminación'"[16]. La ex procuradora general de la Nación sostiene asimismo que tal criterio ha sido adherido por la Corte Suprema de Justicia en fallos como "Urteaga", en el que se sostuvo: "[…] en aquel marco constitucional, no reglamentado aún por el órgano competente, corresponde a este Tribunal delinear los alcances de la garantía mencionada con razonable flexibilidad, a fin de otorgar al peticionario la plena protección que ella establece, sin condicionar el ejercicio de aquella potestad reglamentaria que hasta el presente no ha sido ejercida por el Congreso Nacional".[17] En la misma línea, la académica sostiene que uno de los presupuestos sustanciales para el ejercicio de la acción de hábeas data es el interés legítimo del titular el que debe estar vinculado a la identidad, privacidad, intimidad, honor, reputación o imagen personal[18].

Expuesto lo anterior, podría precipitadamente concluirse que una publicación en Facebook[19] que contenga información personal podría

[15] Ley N.º 25.326, art. 1.

[16] Gils Carbó, ob. cit., p. 244.

[17] CSJN, "Urteaga, Facundo Raúl c/ Estado Nacional - Estado Mayor Conjunto de las FF. AA. s/ amparo ley 16.986", 15/10/1998 (Fallos: 321: 2767).

[18] Gils Carbó, ob. cit., p. 252.

[19] En este ejemplo y tal como se expone en este trabajo, Facebook resulta un responsable de tratamiento y sujeto obligado de la Ley de Protección de Datos Personales toda vez que ejerce un tratamiento de datos en los términos de la ley que lo define en su artículo 2 como: "operaciones y procedimientos sistemáticos, electrónicos o no, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción, y en general el procesamiento de datos personales, así como también su cesión a terceros a través

habilitar el ejercicio del derecho de supresión por el titular de aquellos datos fundamentado en *(i)* la falta o revocación del consentimiento que resulta condición para la recolección legítima de datos personales; *(ii)* el contenido falso, inexacto o discriminatorio; o, incluso, en *(iii)* la afectación a su intimidad. Sin embargo, el mismo texto de la ley que reglamenta el hábeas data, al referir a las excepciones al acogimiento de esta acción, recepta la potencial tensión de derechos que presupone dar curso a esta acción: en su artículo 16 inciso 5 establece que la misma no procederá "[…] cuando pudiese causar perjuicios a derechos o intereses legítimos de terceros, o cuando existiera una obligación legal de conservar los datos".

El Proyecto de Ley de Protección de Datos Personales enviado al Congreso por el Poder Ejecutivo[20] recepta especialmente el derecho bajo análisis. El texto reconoce al titular del dato en primera instancia el derecho de oposición, el que consiste en la facultad del titular de negarse a que sus datos continúen siendo tratados cuando este no haya prestado su consentimiento,[21] y difiere en principio del derecho de supresión. Este último consiste en la facultad de requerir la eliminación de los datos de las bases de datos del responsable del tratamiento, y en tal sentido el proyecto reconoce en el inciso "c" que el titular de datos que ejerce su derecho de oposición podrá requerir la supresión en tanto no prevalezcan otros motivos legítimos para el tratamiento de sus datos. Resulta destacable mencionar que el texto enviado al Congreso reconoce la potencial tensión que introduce estos derechos con la libertad de expresión, siempre que específicamente contemple la excepción a su procedencia en tal fundamento al establecer en el último párrafo del artículo 31: "La supresión tampoco procede cuando el tratamiento de datos sea necesario para ejercer el derecho a la libertad de expresión e información".

En vistas de lo expuesto: ¿es posible solicitar la supresión de un contenido que afecte la intimidad del individuo sobre la base del derecho de

de comunicaciones, consultas, interconexiones o transferencias".

[20] El mensaje se encuentra disponible en: https://bit.ly/2Rhftvs.

[21] Artículo 30. Derecho de oposición. El titular de los datos puede oponerse al tratamiento de sus datos, o de una finalidad específica de éste, cuando no haya prestado consentimiento. El responsable del tratamiento debe dejar de tratar los datos personales objeto de oposición, salvo que existan motivos legítimos para el tratamiento que prevalezcan sobre los derechos del titular de los datos.

cancelación previsto en el hábeas data? ¿Resulta la libertad de expresión fundamento y argumento autosuficiente que permite denegar por defecto dicha solicitud con relación a la publicación de un tercero?

5. Supresión de contenido injurioso en redes sociales

Los cuestionamientos introducidos en el apartado anterior en cuanto a la procedencia del derecho de supresión referido a publicaciones de terceros, no es más que otro supuesto de la contraposición entre el derecho de la intimidad y honra del titular del dato y la libertad de expresión de quien postea tal contenido y quienes tiene acceso al mismo. Dicha tensión de derechos de igual jerarquía constitucional debe resolverse delimitando la legitimidad de la intromisión en la intimidad de los sujetos y teniendo en miras las particularidades del medio digital, tal como sugiere la Declaración Conjunta sobre Libertad de Expresión[22]. En el supuesto de que ambos derechos no se armonicen adecuadamente, la cancelación de contenido podría devenir un supuesto de restricción ilegitima a la libertad de expresión y censura. Al respecto, la Relatoría para la Libertad de Expresión sostiene: "Según la jurisprudencia interamericana, constituyen ejemplos de censura previa, entre otros, los siguientes: la incautación de libros, materiales de imprenta y copias electrónicas de documentos; la prohibición judicial de publicar o divulgar un libro; la prohibición a un funcionario público de realizar comentarios críticos frente a un determinado proceso o institución; en relación con publicaciones en internet, la orden de incluir o retirar determinados enlaces (*links*), o la imposición de determinados contenidos; la prohibición de exhibir una película de cine, o la existencia de una disposición constitucional que establece la censura previa en la producción cinematográfica".[23]

[22] Relator Especial de las Naciones Unidas (ONU) sobre la Promoción y Protección del derecho a la Libertad de Opinión y de Expresión, Representante para la Libertad de los Medios de Comunicación de la Organización para la Seguridad y la Cooperación en Europa (OSCE), Relatora Especial de la Organización de Estados Americanos (OEA) para la Libertad de Expresión, y Relatora Especial sobre Libertad de Expresión y Acceso a la Información de la Comisión Africana de Derechos Humanos y de los Pueblos (CADHP). 1 de junio de 2011. Declaración conjunta sobre libertad de expresión e Internet. Punto 1 (c).

[23] CIDH, *Marco Jurídico Interamericano sobre Libertad de Expresión*, 2009, p. 54, párr. 148

Asimismo, la Comisión Interamericana de Derechos Humano ha expuesto expresamente la problemática de la remoción de contenido al sostener: "La remoción de contenidos en Internet tiene un impacto evidente en el derecho a la libertad de expresión, tanto en su dimensión individual como social, y en el derecho de acceso a la información por parte del público. La información removida no circula, lo que afecta el derecho de las personas a expresarse y difundir sus opiniones e ideas y el derecho de la comunidad a recibir informaciones e ideas de toda índole".[24]

La Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos recuerda que las restricciones del derecho a la libertad de expresión se encuentran contenidas en los artículos 13 (que prevé que el derecho no puede estar sujeto a previa censura sino a responsabilidades ulteriores), 8 (con relación a garantías judiciales) y 25 (con relación a la protección judicial) de la Convención Americana y que los requisitos de tal restricción: "[…] pueden resumirse como (1) consagración legal; (2) búsqueda de una finalidad imperativa; (3) necesidad, idoneidad y proporcionalidad de la medida para alcanzar la finalidad perseguida; (4) garantías judiciales; y (5) satisfacción del debido proceso, incluyendo las notificaciones al usuario".[25] Además, toda restricción a la libertad de expresión, como puede ser la cancelación de una publicación injuriosa, debe ser analizada en el contexto del medio digital y sus particularidades.

En lo que respecta a las particulares del contexto digital, la Relatoría para la Libertad de Expresión sostiene que "[…] es necesario tener en cuenta la disponibilidad de medidas menos restrictivas sobre el derecho a la libertad de pensamiento y expresión que —en Internet— pueden estar más fácilmente disponibles que en entornos analógicos. Así por ejemplo, como ya lo indicó el Relator Especial de las Naciones Unidas sobre la promoción y protección del derecho a la libertad de opinión y de expresión, resulta en extremo relevante atender a la posibilidad de ejercer de

[https://bit.ly/1on89fG].

[24] CIDH, *Informe Anual 2016, Informe de la Relatoría Especial para la Libertad de Expresión*, OEA/Ser.L/V/II, Doc. 22/17, 15/3/2017, p. 443, párr. 133 [https://bit.ly/2ptYbQk].

[25] Relatoría Especial para la Libertad de Expresión Comisión Interamericana de Derechos Humanos, *Libertad de Expresión e Internet*, 2013, p. 28 [https://bit.ly/1iiWETW].

manera más efectiva y veloz el derecho de rectificación o respuesta previsto en el artículo 14 de la Convención Americana"[26]. Teniendo en consideración tal estándar, dar lugar al derecho de cancelación de un contenido injurioso podría resultar en una censura ilegítima desde la perspectiva de la libertad de expresión siempre que existan medidas menos gravosas disponibles, inmediatas y efectivas como el derecho de réplica.

Sin perjuicio de lo anterior, el derecho de réplica ante cierto contenido injurioso y su consecuente afectación al derecho a la intimidad y honra podría no ser suficiente o adecuado, por lo que el derecho a exigir la cancelación debería ser atendido. En este sentido, corresponde destacar que la misma Relatoría, en el documento ya citado, admite mecanismos de filtrado y bloqueo aplicados de forma excepcional ante contenido ilícito que no esté amparado por la libertad de expresión, siempre que se respeten las garantías contempladas en los artículos 8 y 25 de la Convención. En este sentido, el organismo entiende que "En casos excepcionales, cuando se está frente a contenidos abiertamente ilícitos o a discursos no resguardados por el derecho a la libertad de expresión (como la propaganda de guerra y la apología del odio que constituya incitación a la violencia, la incitación directa y pública al genocidio, y la pornografía infantil) resulta admisible la adopción de medidas obligatorias de bloqueo y filtrado de contenidos específicos. En estos casos, la medida debe someterse a un estricto juicio de proporcionalidad y estar cuidadosamente diseñada y claramente limitada de forma tal que no alcance a discursos legítimos que merecen protección. En otras palabras, las medidas de filtrado o bloqueo deben diseñarse y aplicarse de modo tal que impacten, exclusivamente, el contenido reputado ilegítimo, sin afectar otros contenidos".[27]

---

[26] Relator Especial de las Naciones Unidas (ONU) sobre la Promoción y Protección del derecho a la Libertad de Opinión y de Expresión, Representante para la Libertad de los Medios de Comunicación de la Organización para la Seguridad y la Cooperación en Europa (OSCE), Relatora Especial de la Organización de Estados Americanos (OEA) para la Libertad de Expresión, y Relatora Especial sobre Libertad de Expresión y Acceso a la Información de la Comisión Africana de Derechos Humanos y de los Pueblos (CADHP), 1/6/2011, declaración conjunta sobre libertad de expresión e Internet, punto 4 (a), citado en Relatoría Especial para la Libertad de Expresión Comisión Interamericana de Derechos Humanos, *Libertad de Expresión e Internet*, 2013, p. 32.

[27] Relatoría Especial para la Libertad de Expresión Comisión Interamericana de Derechos

En vistas de lo expuesto, lo que resulta claro es que no toda intromisión a la intimidad puede ser reputada legítima en pos de la libertad de expresión, y ante esto existen dos mecanismos admitidos por nuestro ordenamiento jurídico en el marco de Internet y de las redes sociales en particular: *(i)* el derecho de réplica y *(ii)* el derecho a la cancelación o bloqueo del contenido en cuestión. A los efectos de determinar la procedencia del último derecho, deberá analizarse el caso concreto y determinar si *(i)* el contenido está protegido bajo la libertad de expresión y *(ii)* si existen medios alternativos, tales como la réplica, que resulten reparación suficiente y menos gravosas que los efectos de la libertad de expresión. En el supuesto de que ambas condiciones se den, es decir que el contenido esté protegido por la libertad de expresión y existan medios alternativos menos gravosos que la cancelación, nos encontraremos bajo la excepción prevista en el artículo 16 inciso 5[28] de la Ley de Protección de Datos Personales, y corresponderá desestimar la solicitud de supresión del titular del dato. Este test guarda relación con el test tripartito tripartido desarrollado por la jurisprudencia y doctrina interamericana el cual sostiene que toda limitación a la libertad de expresión debe *(i)* estar legalmente establecida en una ley en sentido formal y material, *(ii)* debe ser necesaria e idónea y *(iii)* proporcional[29].

Independientemente de la adopción de cualquiera de los mecanismos referidos en el párrafo anterior, todo procedimiento deberá respetar las garantías constitucionales e impuestas por la Convención Americana de Derechos Humanos, a tal efecto y en caso de corresponder la cancelación de contenido, deberá notificarse de la misma al editor o autor de tal contenido a fin de garantizar su derecho a realizar su descargo y recurrir la decisión.

Adicionalmente, resulta destacable reiterar que la proporcionalidad, necesidad o idoneidad de la cancelación de contenido deberá contemplar el particular medio en el cual tal contenido está inserto. Tal como se ade-

Humanos. *Libertad de Expresión e Internet*, 2013, p. 40, párr. 85 [https://bit.ly/1iiWETW].

[28] Ley N.º 25.326, art. 16 inc. 5: "La supresión no procede cuando pudiese causar perjuicios a derechos o intereses legítimos de terceros, o cuando existiera una obligación legal de conservar los datos".

[29] Relatoría Especial para la Libertad de Expresión Comisión Interamericana de Derechos Humanos, *Libertad de Expresión e Internet*, 2013, p. 28 [https://bit.ly/1iiWETW].

lantó, las redes sociales como Facebook permiten ejercer un derecho de réplica instantáneo e irrestricto, por lo que dicha dinámica del discurso, por ejemplo, será un vector clave para la decisión.

Establecer criterios absolutos para la determinación de la afectación ilegítima al derecho a la intimidad y la honra resultaría arriesgado, toda vez que las particularidades de cada caso podrían llevar a situación injustas y hacer peligrar la libertad de expresión, tal como se refirió en el caso "Kimel"[30] resuelto por la Corte Interamericana de Derechos Humanos. No obstante, el derrotero jurisprudencial ha permitido establecer cierto estándar de aplicación que permitiría dilucidar aquel supuesto de "abuso de libertad de expresión" y de intromisión ilegítima al derecho a la intimidad. Al respecto, la Comisión Interamericana de Derechos Humanos ha reforzado que los siguientes discursos tienen especial protección bajo la libertad de Expresión: "*(a)* el discurso político y sobre asuntos de interés público; *(b)* el discurso sobre funcionarios públicos en ejercicio de sus funciones y sobre candidatos a ocupar cargos públicos; y *(c)* el discurso que configura un elemento de la identidad o la dignidad personales de quien se expresa".[31]

En la misma línea anterior, la Corte Interamericana se ha pronunciado reiteradamente acerca del umbral distinto de protección de la intimidad de los funcionarios públicos o de aquellas personas que importan al debate de una sociedad democrática, afirmando que dichos sujetos deberán tolerar ciertas intromisiones a su intimidad o afectaciones a su honra o a su reputación en pos del interés público,[32] todo aquello en virtud de que "[…] se justifica por el carácter de interés público de las actividades que realizan; porque se han expuesto voluntariamente a un escrutinio más exigente; porque sus actividades trascienden la esfera privada para ingresar a la esfera del debate

[30] "Kimel v. Argentina", CIDH, 2/5/2008.

[31] *Informe Anual de la Comisión Interamericana de Derechos Humanos*, 2009, p. 232 [https://bit.ly/1qZ9spq].

[32] CIDH, caso "Kimel v. Argentina", sentencia de 2/5/2008, serie C N.º 177, párr. 86 y 87; CIDH, Caso Palamara Iribarne v. Chile, sentencia de 22/11/2005, serie C N.º 135, párr. 83 y 84; CIDH, Caso Herrera Ulloa v. Costa Rica", sentencia de 2 de julio de 2004, serie C N.º 107, párr. 128 y 129; CIDH, caso "Tristán Donoso v. Panamá", excepción preliminar, fondo, reparaciones y costas, sentencia de 27/1/2009, serie C N.º 193, párr. 115; CIDH, *Informe Anual 1994*, cap. V: Informe sobre la Compatibilidad entre las Leyes de Desacato y la Convención Americana sobre Derechos Humanos, tít. IV, OEA/Ser. L/V/II.88. doc. 9 rev. 17/2/1995.

público; y porque cuentan con medios apropiados para defenderse".[33]

La Corte Suprema de Justicia de la Nación también ha reconocido un criterio flexible para aquellos sujetos cuya afectación a la intimidad se corresponde al debate público y la vida en democracia. Asimismo, el máximo tribunal sostiene la doctrina de la "expectativa de privacidad" que refiere a la congruencia del comportamiento de quien reputa una afectación a su intimidad. La mencionada doctrina fue sentada en el fallo "Ponzetti de Balbín",[34] en el cual se sostuvo: "Que en el caso de personajes célebres cuya vida tiene carácter público o personajes populares, su actuación pública o privada puede divulgarse en lo que se relacione con la actividad que les confiere prestigio o notoriedad y siempre que lo justifique el interés general. Pero ese avance sobre la intimidad no autoriza a dañar la imagen pública o el honor de estas personas y menos sostener que no tienen un sector o ámbito de vida privada protegida de toda intromisión. Máxime cuando con su conducta a lo largo de su vida no ha fomentado las indiscreciones ni por propia acción, autorizado, tácita o expresamente la invasión a su privacidad y la violación al derecho a su vida privada en cualquiera de sus manifestaciones".[35]

En vistas de lo anterior, en el marco de redes sociales como Facebook, reputar un contenido publicado por un tercero como una intromisión ilegítima a la intimidad de los individuos que concluya en la admisión de una medida tal como la cancelación del contenido en principio resulta excepcional y reservado para discursos no protegidos (como el caso de los referidos discursos de odio o pornografía infantil, entre otros). Lo anterior, en tanto la cancelación del contenido, presupone una afectación a la libertad de expresión que *(i)* constituye la excepción a la procedencia del derecho de cancelación contenida en el artículo 16 inciso 5 de la Ley de Protección de Datos Personales y *(ii)* exige un escrutinio estricto que preferencia medidas menos restrictivas como el derecho de réplica, el que en un entorno de redes sociales como Facebook se encuentra garan-

[33] Relatoría Especial para la Libertad de Expresión Comisión Interamericana de Derechos Humanos, *Marco jurídico interamericano sobre el derecho a la libertad de expresión*, 2010, p. 41 [https://bit.ly/1on89fG].

[34] CSJN, "Ponzetti de Balbín, Indalia c/ Editorial Atlántida S. A. s/ daños y perjuicios", 11/12/84 (Fallos: 306: 1892).

[35] Ibíd. considerando 9.

tizado en la dinámica propia de tal plataforma. En cuanto al escrutinio, corresponderá analizar quién resulta competente para atender tal tarea: ¿se debe entender reservada solo a un juez? ¿Es la autoridad de control competente para encomendarse en tal tarea en el marco de su objetivo de velar por el cumplimiento de la Ley de Protección de Datos Personales y su facultad de sanción?

6. La Agencia de Acceso a la Información Pública y su competencia

El 7 de febrero de 2011 la Dirección Nacional de Protección de Datos Personales emitió un controversial dictamen[36] en el que entendió que cierto buscador debía bloquear o suprimir los datos relativos a los enlaces que habían sido denunciados por el titular del dato atendiendo así a su derecho de supresión, toda vez que resultara evidente la afectación al derecho a la intimidad del denunciante y de la menor involucrada[37]. Sin perjuicio de este antecedente aislado, y si bien existen varios puntos cuestionables en cuanto a la competencia y legitimidad de la decisión del regulador en ese momento, resulta pertinente analizar si la actual Agencia de Acceso a la Información Pública podría legítimamente expedirse en igual sentido y resolver la tensión de derechos que presupone el derecho a la supresión del afectado en contraposición de la libertad de expresión.

La Agencia de Acceso a la Información Pública es un órgano creado por la Ley N.º 27.275 a la cual se lo asignó como Autoridad de Aplicación de la Ley de Protección de Datos Personales a través del Decreto N.º 746/2017. En cuanto a su competencia, está regulada en el capítulo V de la Ley N.º 25.326, en el que se dispone que el órgano de control "[…] deberá realizar todas las acciones necesarias para el cumplimiento de los objetivos y demás disposiciones de la ley". A los efectos de lo anterior, el inciso "f" establece como función y atribución "Imponer las sanciones administrativas que en su caso correspondan por violación a las normas

[36] Dictamen DNPDP N.º 3/11.

[37] Google Inc. judicializó la decisión en 2012 reclamando la nulidad del acto administrativo obteniendo una sentencia desfavorable en primera instancia, la que sería revocada por la Cámara de Apelaciones en los Contencioso Administrativo Federal. La decisión de la Cámara se centra en que el titular de los datos que inició el reclamo no había tenido intervención en el procedimiento. "Google Inc. c/ DNPDP-DISP 3/11 s/ Proceso de Conocimiento", CAF, 2/6/2015.

de la presente ley y de las reglamentaciones que se dicten en su consecuencia". En vistas del marco regulatorio referido, podría primeramente arribarse a la conclusión de que la Agencia de Acceso a la Información se encuentra facultada a establecer sanciones en supuestos de incumplimiento mas no ordenar otro tipo de medidas, como aquellas relacionadas a la reparación de un derecho vulnerado.

Sin perjuicio de lo anterior, la legalidad de una orden de supresión de contenido debe evaluarse desde la perspectiva constitucional y de los convenios internacionales. En este sentido, el artículo 116 de la Constitución Nacional expresamente establece que le corresponde al Poder Judicial tomar conocimiento y decidir sobre los puntos regidos en ella. En el marco del texto constitucional, parece indicarse que la tensión entre el derecho a la libertad de expresión y el derecho a la intimidad que presupone la solicitud de cancelación de amparado en la Ley N.º 25.326 debe ser decidida por un juez competente, mas no por otro organismo.

Asimismo, y en línea con lo ya expuesto, la Comisión Interamericana ha sostenido que la orden de cancelación de contenido —o la imposición de sanciones por no acatar tal orden de cancelación— es una censura a la libertad de expresión[38] que debe entonces ser armonizada con el mandato constitucional que garantiza la libertad de expresión sin censura previa. A los efectos de determinar la legitimidad de tal censura, deberá aplicarse el test tripartito referenciado en el apartado anterior (la medida debe estar prevista en una ley en sentido formal y material; debe ser necesaria e idónea y proporcional). Además, el organismo ha sostenido que tales limitaciones deberán ser ordenadas por un juez o autoridad jurisdiccional competente, independiente e imparcial, atendiendo a todas las garantías del debido proceso[39].

En la misma línea, grupos de la sociedad civil de todo el mundo han desarrollado una serie de principios, denominados Principios Manila,[40]

[38] CIDH, *Marco Jurídico Interamericano sobre Libertad de Expresión*, 2009, p. 54, párr. 148 [https://bit.ly/1on89fG].

[39] CIDH, *Informe Anual 2016. Informe de la Relatoría Especial para la Libertad de Expresión*, OEA/Ser.L/V/II. Doc. 22/17, 15/3/2017, p. 444, párr. N.º 135.

[40] Los Principios Manila fueron presentaron en Manila, Filipinas, en 2015, en el marco de la convención mundial de derechos humanos en la era digital RightsCon. Los principios han sido desarrollados por múltiples organizaciones defensores de derechos humanos del mundo como

a fin de asegurar garantías mínimas y buenas prácticas para establecer responsabilidad de intermediarios. Tales principios se basan en instrumentos internacionales sobre derechos humanos y otros marcos legales internacionales. Entre estos principios, han enumerado el siguiente: "Los intermediarios no deben ser obligados a restringir contenidos a menos que una orden emitida por una autoridad judicial independiente e imparcial haya determinado que el contenido en cuestión es ilícito".[41]

La competencia exclusiva del Poder Judicial a fin de expedirse en cuanto a la baja de contenidos tiene un fuerte sustento en *(i)* la independencia de este organismo y en que *(ii)* son los jueces quienes se encuentran en mejor situación para evaluar los daños y determinar las medidas consecuentes, realizando el escrutinio necesario para resolver la tensión de derechos entre la libertad de expresión y el derecho a la intimidad, velando por las garantías de ambas partes.

En vistas del marco antes expuesto, difícilmente pueda concluirse que un organismo como la Agencia de Acceso a la Información Pública pueda reputarse legítimo para decidir restricciones a la libertad de expresión, como presupone la determinación de la procedencia del derecho de cancelación de contenido en fundamentado a la Ley de Protección de Datos Personales. Lo anterior, en tanto el mismo artículo 16 de la Constitución Nacional le otorga la facultad jurisdiccional al Poder Judicial a fin de entender en cuestiones como la que presupone la armonización de derechos constitucionales en un caso particular y que no se encuentran dadas la garantía de independencia referida por los organismos internacionales.

En relación con la independencia de la Agencia de Acceso a la Información Pública resulta pertinente remarcar que *(i)* si bien la Ley de Acceso la Información Pública le ha dado carácter autárquico, el Decreto

Electronic Frontier Foundation (Estados Unidos), Fundación Karisma (Colombia), Heliopolis Institute (Egipto), Social Media Exchange (Líbano), International Alliance on Information for All (Reino Unido),Greenhost (Países Bajos), The Association for Freedom of Thought and Expression (AFTE), Filipino Freethinkers (Filipinas), Comunes Collective (España), FLOSSK (Albania), Hiperderecho (Perú), article 19, ONG Derechos Digitales (Chile), Free Press (Estados Unidos) y el Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE) (Argentina), entre otros.

[41] Segundo Principio Manila [www.manilaprinciples.org/es].

Reglamentario ha establecido su dependencia a la Jefatura de Gabinete, lo cual potencialmente puede representar un conflicto de interés a fin de asegurar la libertad de expresión en cuanto a discursos que refieran al poder político, y *(ii)* su presupuesto, si bien autónomo, se encuentra determinado por el Poder Ejecutivo[42].

Sin perjuicio de lo anterior, no debería apresuradamente concluirse que ninguna autoridad independiente no judicial no sea idónea para resolver la tensión descripta bajo regímenes jurídicos foráneos. Con relación a este punto, resulta pertinente resaltar que el Reglamento General de Protección de Datos Personales europeo prevé la creación de autoridades de control independientes que en principio tendrían facultades para resolver estas cuestiones[43]. En tal sentido, el reglamento referido establece ciertos principios a los efectos de velar por la independencia de tal autoridad bajo el artículo 52 y establece entre sus facultades de sanción la potestad de ordenar la supresión de datos personales,[44] siempre que esta resulte procedente dentro de los límites del mismo reglamento. Al respecto, corresponde recordar que el apartado 3 del artículo 17 del reglamento establece el supuesto de afectación a la libertad de expresión como excepción al ejercicio del derecho de supresión. En igual sentido se puede citar el caso de México, quien ha garantizado la independencia de la autoridad de control (el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales) a través del artículo 6 de la Constitución Política de los Estados Unidos Mexicanos al establecer la creación de un órgano "[…] autónomo, especializado, imparcial, colegiado, con personalidad jurídica y patrimonio propio, con plena autonomía técnica, de gestión, capacidad para decidir sobre el ejercicio de su presupuesto y determinar su organización interna, responsable de garantizar el cumplimiento del derecho de acceso a la información pública y a la protección de datos personales en pose-

[42] Con relación a este punto resulta pertinente señalar el recorte de presupuesto del organismo dictada a través de la Decisión Administrativa N.º 6/2018. A través de tal decisión el Poder Ejecutivo redujo significativamente el presupuesto aprobado para tal organismo en la Ley de Presupuesto aprobada por el Congreso. Dicha situación resulta un ilustrativo ejemplo de la fragilidad de la independencia de este organismo.

[43] Capítulo VII del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo.

[44] Art. 58, apart. 2, inc. "f" del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo.

sión de los sujetos obligados en los términos que establezca la ley".[45] Por su parte, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, en su capítulo VII, delimita un específico procedimiento que la autoridad deberá seguir ante reclamos de titulares de datos por requerimientos de acceso, rectificación, cancelación u oposición no atendidos por el responsable del tratamiento. Tal procedimiento incluye la oportunidad de descargo del responsable y la acreditación de prueba en forma previa al dictamen de la autoridad acerca de la procedencia del requerimiento[46].

El razonamiento expuesto y la descripción de la problemática que plantea la potencial competencia de la Agencia de Acceso a la Información Pública para atender y resolver esta tensión de derechos, parece haber sido receptada por la redacción del Proyecto de Ley de Protección de Datos Personales enviada al Congreso por el Poder Ejecutivo. En tal sentido, el último párrafo del artículo 77 que refiere a las facultades sancionatorias de la autoridad de control establece: "En ningún caso, estas medidas podrán afectar el derecho a la libertad de expresión e información". Esto representa una limitación a la competencia del regulador, quien deberá analizar este extremo al momento de decidir e incluso deberá interpretar si su competencia comprende decisiones acerca de limitaciones legítimas a la libertad de expresión —en tanto aún tal limitación legítima podría interpretarse como un supuesto de afectación a la libertad de expresión vedado por el texto referenciado—.

7. Términos y condiciones y derechos constitucionales

Adicionalmente este trabajo se propuso analizar si plataformas como Facebook presentan un mecanismo de autorregulación que permita garantizar el ejercicio de los derechos relacionados con la autodeterminación informativa. En este sentido, resulta interesante analizar los términos propuestos que regulan la actividad dentro del entorno de la plataforma que en principio circunscriben la relación entre la plataforma y los usuarios.

[45] Constitución Política de los Estados Unidos Mexicanos, art. 6, ap. A, punto VII [https://bit.ly/2PH7E1i].

[46] Ley Federal de Protección de Datos Personales en Posesión de los Particulares, cap. VIII [https://bit.ly/1vauawz].

Los términos de uso de Facebook[47] describen el tratamiento de datos personales por parte de la empresa y regulan los derechos de acceso, rectificación y supresión de los titulares de datos que utilizan la plataforma. La política de privacidad puntualmente establece la facultad de ejercer el derecho de supresión siempre que tales datos hayan sido recolectados por la plataforma directamente del titular del dato, pero no hay un procedimiento claro ante el supuesto en el que los datos del titular sean provistos por un tercero —como sería el caso en el cual un tercero postea el contenido—. Aún más, la plataforma señala que alguna información no será eliminada si es que un tercero es detentatario[48]. En resumen, los términos de Facebook parecen señalar que difícilmente podría requerirse exitosamente la supresión de un dato personal, como el de la propia imagen, si es que fue posteada por un tercero.

Con relación a lo anterior, debemos recordar que el derecho de supresión no procede en el supuesto en que se afecten derechos de terceros y que dar curso a la supresión del contenido editado o publicado por un tercero podría significar afectar la libertad de expresión, no solo del autor sino de todos los que tienen derecho a acceder al contenido. En vistas de aquello y tal como se expuso en apartados anteriores, resolver tal tensión de derechos no resulta tarea sencilla.

El mecanismo propuesto por la referida plataforma para hacer lugar a potenciales reclamos de intromisión ilegítima a la intimidad, o de contenido injuriante en particular, consiste en un formulario de reporte con relación al reputado contenido. La solicitud será resuelta por un equipo interno de la empresa que evaluará los intereses contrapuestos y concluirá moderando el contenido[49]. Ante tal mecanismo, se abren ciertos cuestionamientos con relación a la facultad del responsable de la plataforma de decidir sobre los discursos y los riesgos para la libre expresión

[47] Se analizó esta plataforma por ser la red social con mayor número de usuarios activos en el mundo. Estadística disponible en: https://bit.ly/2DMf7Gb.

[48] Condiciones de Uso de Facebook: "No se eliminará la información sobre ti que otros compartieron porque no forma parte de tu cuenta" [https://bit.ly/1cwZ2RJ].

[49] Ver capítulo de reportes y denuncias en Condiciones de Uso: https://www.facebook.com/legal/terms. Con relación a este punto resulta interesante el análisis sobre los reportes de trasparencia de Facebook en los que se refiere a la metodología utilizada para la decisión de remoción de contenido [https://bit.ly/2IohhSu].

que presuponen estos mecanismos de autorregulación que en definitiva moderan y delimitan contenidos.

Sin perjuicio de lo anteriormente descripto y de la decisión de la empresa en el marco del mecanismo de autorregulación propuesto, el derecho de supresión previsto en la normativa legal no deberá entenderse agotado en tal procedimiento, siempre que el titular del dato podrá perseguir su derecho de acuerdo con las vías legales previstas en el marco jurídico.

8. Conclusiones

En vistas de los puntos desarrollados en este trabajo, podría concluirse que el marco jurídico argentino vigente, así como el Proyecto de Ley de Protección de Datos Personales,[50] admitiría el ejercicio del derecho de supresión con relación a contenidos publicados por terceros en redes sociales, siempre que su procedencia *(i)* no afecte ilegítimamente la libertad de expresión, *(ii)* se vele por las garantías constitucionales y *(iii)* sea así ordenado por una autoridad judicial competente.

[50] En: https://bit.ly/2Rhftvs.

Procedimiento de resolución de oposiciones marcarias en sede administrativa

por Pablo A. Palazzi

1. Introducción

A comienzos del año 2018 el decreto de necesidad y urgencia (DNU) N.º 27/2018 reformó la Ley de Marcas con el objetivo, entre otros, de "acelerar los tiempos de registro marcario". En junio de 2018 el Congreso aprobó la Ley de Simplificación y Desburocratización para el Desarrollo Productivo de la Nación N.º 27.444, que reproduce sin alteración el texto del DNU con relación a las reformas a la leyes de marcas, patentes y modelos y diseños industriales. Uno de los cambios más importantes de esta reforma es que la resolución de oposiciones marcarias ya no estará en cabeza de los tribunales federales sino en sede administrativa, con la posibilidad de un recurso directo a la Cámara Civil y Comercial Federal.

El 18 de junio de 2018 el Instituto Nacional de la Propiedad Industrial (INPI) publicó la Resolución INPI P-183/18 que aprueba el reglamento de resolución de oposiciones en sede administrativa (en adelante, el Reglamento). La resolución contiene dos anexos. El primero, con sólo once artículos, es el Reglamento para la instancia administrativa de resolución de oposiciones. El segundo anexo contiene los aranceles a aplicar al procedimiento que son básicamente dos: la tasa para mantener la oposición y la tasa para el recurso directo de apelación.

El objeto de este artículo es analizar brevemente los aspectos centrales del nuevo Reglamento para la instancia administrativa de resolución de oposiciones marcarias. Esta nota se basa en el artículo publicado en el diario *La Ley* en noviembre de 2018 pero le hemos agregado comentarios con relación al decreto reglamentario N.º 242/2019.

2. El cambio de paradigma en el sistema de oposiciones

El INPI propuso esta reforma con el objeto de acelerar el procedimiento de registro de marcas. En numerosos sistemas del Derecho Com-

parado, las oposiciones (así como también las caducidades y nulidades) son resueltas en sede administrativa y luego existe la posibilidad de su revisión judicial mediante un recurso directo. Desde una perspectiva de Derecho Comparado, la reforma es entonces positiva pues implica plegarse a las tendencias internacionales que en principio evitan el litigio judicial de oposiciones por considerarlo costoso y complicado[1].

La forma en que se lidiaba con las oposiciones bajo el régimen anterior de alguna manera siempre retrasaba el registro de las marcas que recibían esta clase de objeciones.

En la Argentina, hasta la reforma de la Ley N.º 27.444 las oposiciones, en caso de no existir acuerdo con el oponente para su levantamiento, tenían que ser resueltas judicialmente.

La resolución judicial de oposiciones tuvo lugar tanto bajo la Ley N.º 3.975 (aprobada en noviembre del año 1900) como bajo la Ley N.º 22.362, vigente desde la década de 1980. Por lo tanto los tribunales argentinos llevan más de un siglo resolviendo oposiciones marcarias. Todo esto era algo a lo que los abogados de marcas y agentes de propiedad industrial estaban acostumbrados.

Pero el trámite judicial de cese de oposición podía dilatar extensamente el registro de un signo distintivo, incluso hasta por varios años, incrementando el costo de obtención de una marca en la Argentina. Veamos por qué sucedía esto para entender mejor el porqué de la reforma de la Ley N.º 27.444.

Para lograr levantar la oposición, el solicitante de la marca y el oponente recorrían un largo camino. Para empezar, luego de presentada la oposición, esta tenía que ser notificada al solicitante para poder contar el plazo de un año para levantarla. De conformidad con el reglamento de la Ley de Marcas, el solicitante tenía dos meses para retirar los fundamentos de la oposición una vez notificados y a partir de allí se contaba el año[2]. Es decir que, en la práctica, las partes tenían doce meses, más

[1] Kur, Annette y Martin Senftleben, *European Trademark Law. A commentary*, Oxford, 2017, p. 565.

[2] Artículo15 del decreto 1141/2003: "Vencido el término previsto en el artículo 13 de la ley, la Autoridad de Aplicación notificará al solicitante, mediante publicación en el Boletín de Marcas, de la existencia de oposiciones, de antecedentes y demás objeciones que pudieran obstar al registro de la marca solicitada, debiendo concurrir el solicitante ante la Autoridad de Aplicación, dentro de los 60 días corridos, contados a partir de la fecha de publicación, a los efectos de obtener el

dos meses, más el tiempo que le llevaba al INPI cargar la oposición en el sistema y notificarla por su publicación en el boletín (aproximadamente, de dos a cinco meses). Las partes podían comenzar a negociar el retiro de la oposición antes de ser notificadas, pero en general ello no sucedía de inmediato, pues no había ningún vencimiento inminente. Además el oponente no tenía ningún incentivo para arreglar el caso: si no se llegaba a un acuerdo con el solicitante (o este no iniciaba una demanda de cese de oposición), la solicitud caía en el abandono. Toda la carga de negociar el levantamiento de la oposición recaía sobre el solicitante de la marca. Algunos casos se cerraban en pocos meses, pero la mayoría se negociaba por todo el plazo o incluso hasta último momento.

Si no se llegaba a un acuerdo dentro del término de un año, el paso siguiente era la mediación que tenía que ser solicitada dentro del año antes del vencimiento del plazo. Si la mediación no se cerraba con un acuerdo de partes, el solicitante de la marca tenía que ir a un juicio ordinario y obtener una sentencia de un juez que indicara que la marca solicitada no era confundible con la del oponente (también se podía solucionar con acuerdo de partes). El litigio podía durar entre dos y cinco años (a veces mucho más cuando existían varias marcas, varios oponentes o demandas cruzadas). Superado el juicio, el tribunal informaba al INPI el resultado para que el INPI pudiera seguir el procedimiento de registro, generalmente para realizar el examen de fondo y concediera la marca en caso de considerar que no existía confundibilidad y que la oposición era infundada.

Como es dable advertir, esto demoraba ampliamente el registro de una marca, lo cual es totalmente contrario a la necesidad de celeridad que tiene un empresario que desea lanzar un producto o servicio al mercado y precisa registrar un signo distintivo que lo ampare.

A esto se suma que el sistema argentino de oposiciones permitía y permite presentar una oposición por una gran amplitud de fundamentos. Esto es muy positivo y ayuda a los titulares de propiedad intelectual e industrial a amparar sus derechos. Pero a veces había un abuso de este derecho, porque el criterio de confundibilidad que los agentes de pro-

detalle de las objeciones y antecedentes o, en su caso, de las copias de los escritos de oposición. El plazo de 1 año previsto en el artículo 16 de la ley que se reglamenta, comenzará a correr a partir del vencimiento de este último término, respecto de la totalidad de las oposiciones deducidas".

piedad industrial emplean para determinar la necesidad de presentar una oposición era y es muy generoso. En función de ello, se presentaban y se presentan oposiciones que a veces no tienen fundamento en confusión alguna. Esto obligaba al solicitante a negociar con el oponente y aceptar alguna clase de acuerdo, porque la alternativa a no negociar era un costoso y extenso juicio de conocimiento en la justicia civil y comercial federal. Es por ello que el número de oposiciones es muy alto si se lo compara con otras jurisdicciones. En los últimos dos años el INPI informó que se presentaron entre 15.000 y 16.000 oposiciones por año. Según información facilitada por Damlong, el total de marcas presentadas en el INPI fue de 74.649 en 2017, de 70.907 en 2016 y de 65.651 en 2015. Esto significa que aproximadamente entre un 20% y un 25% de las marcas recibía oposiciones, esto es, una de cada cuatro marcas[3].

Se calcula que del total de oposiciones presentadas, solo el 5% terminaba en una mediación y luego en un juicio,[4] el resto —es decir, el 95%— terminaba en declaraciones de abandono del INPI. Esto tenía muchas causales: posiblemente la oposición era insalvable o la solicitud caía en el abandono por falta de seguimiento del solicitante. En muchos casos se trataba de un particular que no estaba representado por agente de la propiedad industrial o que no podía afrontar los costos de un abogado, una mediación y un extenso juicio de conocimiento para lograr el cese de oposición al registro de marca.

Con el nuevo sistema de resolución administrativa de oposiciones impuesto por la Ley N.º 27.444, la declaración de abandono de una marca por no levantar una oposición no existe más[5]. Es decir, la solicitud

[3] El porcentaje argentino es alto si se lo compara con el existente en Europa. Según un estudio del Instituto Max-Planck para la propiedad intelectual y el derecho de la competencia, los porcentajes de oposiciones en la Unión Europea son muchos más bajos. Por ejemplo, en Dinamarca, las oposiciones sólo representaban entre el 3% de las marcas publicadas, en Francia solo el 6%, en Portugal el 10% y en Eslovenia un 12%. Ver MPI, *Study on the Overall Functioning of the European Trademark System*, p. 12.

[4] Se calcula que en la mediación se resolvía favorablemente con un acuerdo entre el 60% y el 70% de los conflictos, el resto obligaba al solicitante a ir a un litigio judicial o perder la marca por la declaración de abandono del INPI.

[5] El texto original del artículo 16 de la Ley de Marcas decía: "Cumplido un (1) año contado a partir de la notificación prevista en el artículo 15, se declarará el *abandono* de la solicitud en los siguientes casos […]". Con la reforma de la Ley N.º 27.444 desaparece el abandono pues el nuevo texto del artículo 16 dice: "Cumplidos tres (3) meses contados a partir de la notificación de

de marca ya no es declarada abandonada por no impulsar el solicitante una negociación, una mediación o un juicio. Ahora es el oponente quien debe impulsar el proceso de oposición pagando la tasa y ampliando fundamentos. Si las partes no acuerdan nada, el INPI decide si la oposición es o no fundada, siempre que se abra el proceso mediante el pago de una tasa adicional. De lo contrario, si no hay otras oposiciones, el INPI analiza si la marca debe ser o no concedida.

Como es dable observar, esta reforma legal ha debilitado considerablemente el efecto que tenía presentar una oposición: para el solicitante ya no hay más riesgo de perder la solicitud de marca por no negociar, y el oponente debe pagar una tasa adicional para mantener la oposición. Se ha quitado la carga que recaía sobre el solicitante de la marca que implicaba negociar un acuerdo, ir a mediación, y si no lograba un acuerdo, ir a litigar el caso en tribunales para evitar que se declare el abandono de su solicitud.

Pese a los cambios de la Ley N.º 27.444, la resolución de una oposición marcaria sigue siendo un proceso entre dos partes: el solicitante de la marca y el oponente[6]. El INPI no es parte sino que es la autoridad que decide si la oposición está o no fundada, pero no será parte apelada en el recurso directo, ya que no se trata de una revisión del acto administrativo del INPI sino de un ataque a la oposición que se consideró fundada o infundada en los argumentos del oponente.

3. Análisis de la Resolución INPI P-183/18

3.1. Cuestiones generales

3.1.1. Vigencia

La resolución INPI P-183/2018 fue publicada en el Boletín Oficial el 19/7/2018. El artículo 6 de la Resolución P-183 dispone: "Fíjase la

las oposiciones previstas en el artículo 15, si el solicitante no hubiese obtenido el levantamiento de las oposiciones, la Dirección Nacional de Marcas resolverá en instancia administrativa las oposiciones que aún permanezcan vigentes".

[6] Estos fue ratificado por el decreto 242/2019 que al reglamentar el recurso directo previsto en el artículo 17 aclara: "El recurso directo previsto en el presente artículo tramitará solo entre solicitante y oponente" (artículo 17, dec. 242/2019).

vigencia de la presente a partir de los 60 días corridos contados desde su publicación oficial", con lo cual su entrada en vigencia fue el 17 de septiembre de 2018. A su vez, en octubre de 2018 el INPI comenzó a notificar las oposiciones bajo el nuevo régimen. En esos casos ya comenzó entonces a correr el plazo de quince días para mantener la oposición, ampliar fundamentos e impulsar el procedimiento.

Por otra parte, el reglamento de oposiciones se aplica a todas las oposiciones presentadas con posterioridad al 12 de enero de 2018, fecha de entrada en vigencia del DNU 27/2018 (reemplazado luego por la Ley N.º 27.444).

3.1.2. Competencia del INPI para dictar el Reglamento P-183/2018

El INPI tiene competencia en dictar este reglamento en virtud de lo dispuesto en los artículos 16, 17 y 47 de la Ley de marcas (LM), según la reforma de la Ley N.º 27.444.

El nuevo artículo 16 de la LM dispone que si dentro de los tres meses el solicitante no obtiene el levantamiento de la o las oposiciones a su marca, le corresponderá al INPI resolverlas en sede administrativa.

El nuevo artículo 17 de la LM autoriza al INPI a fijar el procedimiento para resolver las oposiciones marcarias.

Finalmente, el nuevo artículo 47 faculta al INPI a dictar la normativa complementaria de la Ley de Marcas "en cuanto al procedimiento del registro de marcas, en todo aquello que facilite el mismo, elimine requisitos que se tornen obsoletos, aceleren y simplifiquen el trámite de registro. A tal efecto podrá, entre otras, modificar el procedimiento descripto en la sección segunda de la presente ley; limitar el examen de las solicitudes a las prohibiciones absolutas o que se relacionen con el orden público, supeditando las relativas a su planteamiento por terceros […]".

Estas tres normas citadas de la Ley de Marcas (según la reforma por la Ley N.º 27.444) autorizan al INPI a reglamentar la forma de resolver las oposiciones en sede administrativa. En ejercicio de esa facultad el INPI dictó el reglamento que comentamos seguidamente.

Con posterioridad al dictado del Reglamento se aprobó el decreto reglamentario de la Ley de Marcas, cuyo artículo 14 ratifica esta compe-

tencia del INPI al disponer: "La Autoridad de Aplicación determinará la forma, contenido y requisitos de las oposiciones, como así también el procedimiento para resolverlas".

3.1.3. Aspectos generales del procedimiento administrativo

Hay que entender la reforma de la Ley N.º 27.444 en perspectiva. Como ya explicamos, con anterioridad a la reforma de la Ley de Marcas las oposiciones se litigaban en sede judicial mediante un juicio ordinario. En la mayoría de los casos esto implicaba transitar dos instancias judiciales completas, con ofrecimiento y producción de toda clase de prueba y su revisión plena en la alzada.

Con la reforma de la Ley N.º 27.444 y su reglamentación a través de la Resolución P-138/2018, este largo proceso fue reemplazado por un procedimiento administrativo con prueba más acotada, y cuyo principal objetivo es la celeridad en la concesión de la marca.

Así el artículo 17 de la Ley de Marcas autoriza al INPI a reglamentar el procedimiento para resolver las oposiciones y aclara que "el procedimiento deberá receptar los principios de celeridad, sencillez y economía procesal".

En tal sentido, los considerandos de la Resolución 138 expresan: "por tratarse de una vía propia de este Reglamento, no le serán de aplicación las vías recursivas previstas en el Título VIII Reglamento de la Ley Nacional de Procedimientos Administrativos t. o. 2017, toda vez que si aquello se permitiera la sencillez, celeridad y economía que se pretende alcanzar, se vería desnaturalizada".

El procedimiento regulado intenta emular al proceso judicial pero no llega a tener todas sus características. Para empezar, se desarrolla en sede administrativa, no en sede judicial. Por esa razón la prueba es más acotada que la que se ofrecía en un juicio ordinario de oposición en sede judicial ya que no se espera que el INPI tenga capacidad de producir pericias o testimoniales.

Asimismo, en sede administrativa no estarán disponibles ciertas defensas típicas del proceso judicial de cese de oposición como las de arraigo, la de incompetencia o la excepción de defecto legal. La ausencia de excepciones previas agiliza el trámite del procedimiento.

Tampoco existe rebeldía en el procedimiento administrativo ni tiene efecto la falta de contestación sobre el reconocimiento de hechos o derechos alegados en la ampliación de fundamentos del oponente. De hecho el solicitante podría no aparecer y resultar victorioso para el caso que el INPI considere la oposición infundada.

Eso sí, a diferencia del proceso judicial, por el principio del informalismo, en teoría cualquiera de las partes pueden presentar una petición en cualquier momento. Por supuesto, atentaría contra la celeridad que se propone en el Reglamento el admitir presentaciones fuera del orden preestablecido en el procedimiento de resolución de oposiciones.

3.1.4. Plazos y celeridad del proceso

Los plazos del reglamento son perentorios e improrrogables con la idea de darle celeridad al procedimiento de resolución de oposiciones.

A los fines de despejar cualquier duda, el artículo 2 de la Resolución 138/2018 establece que "los plazos de días a que alude el presente procedimiento serán considerados días hábiles administrativos, salvo que se especifique que son corridos". Esto coincide con el artículo 1 e) ap. 2 de la Ley N.º 19.549 de Procedimiento Administrativo, que dispone que "en cuanto a los plazos […] se contarán por días hábiles administrativos salvo disposición legal en contrario o habilitación resuelta de oficio o a petición de parte".

La celeridad también queda demostrada por lo dispuesto en otras normas del mismo reglamento. El artículo 7 del Reglamento dispone en forma terminante: "Fuera de la interrupción del plazo establecida en el artículo anterior [se refiere a la posibilidad de mediación], todos los demás plazos del procedimiento que aquí se reglamenta son perentorios y no podrán suspenderse ni prorrogarse. La petición de tomar vista no suspenderá los plazos del presente procedimiento".

Finalmente la celeridad también se evidencia en el nuevo artículo 16 de la LM que establece solo tres meses en lugar de doce meses para finalizar el plazo de negociación de oposiciones.

3.1.5. Recursos

El artículo 4 de la Resolución establece la inaplicabilidad de las vías recursivas previstas en el título VIII del Reglamento de Procedimientos Administrativos (t. o. 2017) al trámite de resolución de oposiciones marcarias en sede administrativa.

El título VIII del Reglamento de Procedimientos Administrativos establece en el artículo 71 el recurso de queja por defectos de tramitación y en el artículo 73 el recurso contra actos de alcance individual y contra actos de alcance general. Finalmente, en el artículo 84 se contempla el recurso de reconsideración, en el artículo 90 el recurso jerárquico y en el artículo 94 el recurso de alzada.

Ninguno de estos recursos está disponible durante el trámite de oposiciones, ya que admitirlos significaría extender el plazo del procedimiento con apelaciones por cualquier motivo.

Asimismo, el artículo 8 del Reglamento dispone que "Los actos administrativos que constituyan providencias simples, y los interlocutorios que dicte la Dirección Nacional de Marcas durante la sustanciación de la instancia administrativa de resolución de oposiciones, incluyendo la resolución final de la misma, no serán susceptibles de impugnación por las vías recursivas previstas en el Reglamento de la Ley Nacional de Procedimientos Administrativos t. o. 2017 y sus modificatorias, *con excepción de las cuestiones relacionadas con el mantenimiento de la vigencia de las oposiciones*". Es decir, el Reglamento deja la puerta abierta para poder apelar la decisión que tuvo por "no mantenida" la oposición, dado que causa un agravio importante implica no abrir el procedimiento de oposiciones. Se entiende que existe la posibilidad de recurrir esta cuestión por la vía recursiva pertinente que exista en la LNPA. Salvo esa excepción prevista en el artículo 8, sólo es apelable la resolución final que se dicta en el procedimiento por la vía del recurso directo.

3.1.6. Aplicación supletoria de la LNPA y del RLNPA

El Reglamento de oposiciones marcarias dispone que serán de aplicación supletoria los artículos 46 a 70 y 106 del Reglamento de la Ley Nacional de Procedimientos Administrativos (RLNPA) y las normas

contenidas en el capítulo V del Código Procesal en lo Civil y Comercial de la Nación en todo aquello que no contradiga el espíritu perseguido por la Ley N.º 27.444 en acortar los plazos de los procedimientos, evitando dilaciones innecesarias y tendiendo a la desburocratización de los trámites seguidos ante el INPI.

Esto se confirma con lo dispuesto en el artículo 47 del decreto reglamentario de la Ley de Marcas, que dispone: "El procedimiento marcario constituye un régimen particular en razón de su especialidad y, como tal, se regula por sus propias disposiciones y por la reglamentación adicional que se dicte. La Ley N.º 19.549 de Procedimiento Administrativo (LNPA) será de aplicación supletoria".

3.1.7. Requisito de patrocinio letrado o de agente de la propiedad industrial

Para registrar una marca no se requiere contar con patrocinio letrado o de agente de la propiedad industrial. Sin embargo, para contestar vistas de fondo sí, de conformidad con la reglamentación vigente. El artículo 3 del Reglamento, siguiendo esa línea, dispone que los escritos del trámite administrativo de resolución de oposiciones deberán contar con patrocinio letrado o de agente de la propiedad industrial. El requisito de patrocinio letrado se fundamenta en lograr un trámite ágil y armónico del procedimiento. También en el hecho que el procedimiento administrativo de oposiciones es especializado. Es el mismo argumento del artículo 56 del CPCC[7] para el proceso civil. El objetivo es que quien no esté asesorado adecuadamente no haga presentaciones que de otro modo entorpecerían el trámite del procedimiento y obligarían a la administración a lidiar con planteos que no se ajusten a las reglas adjetivas o de fondo.

[7] El artículo 56 del CPCC dispone: "Los jueces no proveerán ningún escrito de demanda o excepciones y sus contestaciones, a legados o expresiones de agravios, ni aquéllos en que se promuevan incidentes o se pida nulidad de actuaciones y, en general, los que sustenten o controviertan derechos, ya sea en procesos de jurisdicción voluntaria o contenciosa, si no llevan firma de letrado. No se admitirá tampoco la presentación de pliegos de posiciones ni de interrogatorios que no lleven firma de letrado, ni la promoción de cuestiones, de cualquier naturaleza, en las audiencias, ni su contestación, si la parte que las promueve o contesta no está acompañada de letrado patrocinante".

La consecuencia de esto es que el escrito sin patrocinio (esto es, sin firma de abogado o de agente de la propiedad industrial) se tendrá como no presentado. El INPI deberá correr una vista avisando de esta deficiencia formal y dando tiempo para subsanarlo, dado que ello hace a la defensa en juicio contemplada en la LNPA. Asimismo se debe tener en cuenta que la sanción por falta de patrocinio letrado no está contemplada expresamente en el Reglamento (a diferencia del artículo 57 del CPCC que tiene por no presentado esta clase de escritos).

3.2. Ratificación de la oposición y ampliación de fundamentos

3.2.1. Ratificación de la oposición

El artículo 1 del Reglamento aprobado por la Disposición 138/2018 dispone: "Vencido el plazo de tres (3) meses, la Dirección Nacional de Marcas notificará a los oponentes, que todavía no hayan retirado su oposición, para que dentro del plazo improrrogable de quince (15) días hábiles, mantengan la vigencia de la oposición al registro de la marca abonando el arancel correspondiente a la instancia administrativa de resolución de oposiciones y amplíen, dentro del mismo plazo, los fundamentos que hagan a su derecho, ofreciendo en ese acto las pruebas que estimen pertinentes".

Este es un cambio importante que refleja la intención de los redactores del DNU 27 y de la Ley N.º 27.444 de acelerar el registro de marcas y evitar dilaciones causadas con oposiciones infundadas. En el sistema anterior vigente bajo la Ley N.º 22.362 bastaba presentar la oposición para frenar el trámite del registro de la solicitud de marca y obligar al solicitante a negociar un acuerdo. Esto no es más así, y el oponente ahora debe realizar una serie de pasos adicionales para seguir siendo oponente.

Como ya señalamos, la reforma implica un cambio de paradigma en el sistema de oposiciones. Con la reforma de la Ley N.º 27.444 el oponente es quien impulsa y costea la oposición. Esto implica que se va a tener que comportar como actor e impulsarla manteniendo la oposición, produciendo la prueba, etcétera. En el sistema anterior, luego de presentada la oposición, el oponente podía sentarse a esperar que

lo contactasen para negociar. Si no hacía nada o no negociaba con el solicitante de la marca, su oposición resultaba exitosa porque el INPI resolvía el abandono de la solicitud de marca vencido el plazo legal. Con el nuevo régimen, los roles se invierten: el oponente será el actor en el procedimiento administrativo (en el procedimiento judicial el oponente era el demandado).

La nueva norma claramente indica dos acciones que el oponente debe realizar dentro del plazo de quince días hábiles de notificado:[8] *(i)* mantener la vigencia de la oposición al registro de la marca abonando el arancel correspondiente a la instancia administrativa de resolución de oposiciones y *(ii)* ampliar los fundamentos que hagan a su derecho, ofreciendo en ese acto las pruebas del caso.

Ambos actos deben hacerse dentro del mismo plazo, esto es quince días desde la notificación. Ambos actos pueden hacerse por separado o conjuntamente. El pago de la tasa y el escrito de ampliación es individual por cada oposición. Es decir, si se presentaron diez oposiciones, se deben pagar diez aranceles y hacer diez ampliaciones separadas[9].

La no presentación del pago o su presentación extemporánea implica el abandono de la oposición, la que según el artículo 1 del Reglamento queda transformada en un llamado de atención. Esta solución implementada originalmente por el Reglamento se ratifica con lo dispuesto en el decreto reglamentario de la Ley de Marcas.

El artículo 16 *in fine* del decreto 242/2019 dispone: "Las presentaciones efectuadas fuera del plazo indicado en el artículo 13 de la Ley N.º 22.362 y sus modificaciones, así como también aquellas que no hubiesen

[8] El INPI informó que en principio la notificación será por boletín pero en un futuro se hará por medio de la notificación electrónica a través del sistema del expediente electrónico implementado por el Ministerio de Modernización.

[9] Se espera que el INPI agrupe de hecho las oposiciones contra marcas similares en "grupos de casos" a los fines de ser resueltas por el mismo examinador. Es más, este principio de acumulación debería estar contemplado a futuro en una reforma del reglamento, indicando que en casos de idénticos oponente, solicitante y objeto (marcas opuestas en diferentes clases), las partes podrán realizar una única presentación conjunta que involucre a todas las oposiciones, y el INPI podrá dictar una única resolución para todos los casos agrupados, ahorrando tiempo y recursos a todas las partes. También podría darse un caso de acumulación de casos relacionados a nivel judicial, cuando varios recursos directos sean asignados a la misma sala de la Cámara de Apelaciones en lo Civil y Comercial Federal para evitar que oposiciones similares sean resueltas por diversas salas en forma contradictoria.

pagado la tasa de presentación o de mantenimiento de su vigencia, no darán lugar al procedimiento de oposiciones a que se refiere el artículo 16 de la citada ley, pero podrán ser consideradas por la Dirección Nacional de Marcas del INPI, siempre que el registro de la marca implique una afectación al orden público".

Asimismo, el artículo 47 *in fine* del decreto reglamentario de la Ley de Marcas dispone: "Se tendrá por no presentada toda presentación que carezca del pago de la tasa o arancel correspondiente".

Si no se abona la tasa de mantenimiento de oposición, no se abre la instancia administrativa de resolución de oposiciones. Por lo tanto, el INPI no decide si esa oposición es o no fundada. La solicitud de marca en cuestión pasa a la etapa de análisis de antecedentes (estudio de fondo) y al análisis de concesión (salvo que existan otras oposiciones contra la misma solicitud que sí hayan sido mantenidas). La falta de pago de la tasa implica que no hay interés en proseguir con el trámite de oposición, el oponente deja de ser parte y no puede recurrir una eventual resolución concediendo la marca por los motivos de la oposición.

En el hipotético caso de que por un error el INPI considere que no se mantuvo la oposición cuando ello sí ocurrió, el oponente podrá recurrir esta instancia. En principio las decisiones durante el procedimiento no son recurribles, pero la excepción es la que no tiene por mantenida la oposición según lo prescripto por el artículo 8 *in fine* del Reglamento.

Al establecer la sanción, la norma sólo se refiere al pago, no a la ampliación de fundamentos. En tal sentido, el artículo 1 de la Disposición 138/2018 dispone que "Si el arancel no fuese abonado en término, ello importará la falta de interés del oponente de mantener vigente la oposición, por lo que, automáticamente y sin más trámite no se abrirá la instancia administrativa de oposiciones y será considerada por la Dirección Nacional de Marcas como un mero llamado de atención".

La falta de presentación del escrito de ampliación de fundamentos y ofrecimiento de prueba no implica el desistimiento de la oposición. Bien puede suceder que no sea necesario ampliar argumentos, o que el oponente pudo haber expresado todos sus argumentos y pruebas al presentar la oposición y entender que, con el pago de la tasa, alcanza para mante-

ner la oposición. En síntesis, no es necesario ampliar fundamentos para mantener vivo el trámite de la oposición. Sin embargo, es recomendable hacerlo para estar en mejor posición en caso de tener que presentar un recurso directo ante la justicia.

El formulario de oposición del INPI tiene un limitado espacio donde el oponente sólo tiene lugar para un par de frases. Aunque sería posible presentar documentación y argumentos en una hoja anexa al formulario de oposición, esto no es lo frecuente. Por otra parte, el oponente siempre podía ampliar la oposición luego de presentada con argumentos. Pero ahora la ampliación de fundamentos es el acto expreso mediante el cual se aporta prueba y se desarrollan los argumentos de la oposición. Salvo casos de doble identidad marcaria (misma marca para la misma clase de productos), el resto de los casos usualmente requieren más argumentación y en algunos casos extensa prueba.

El reglamento contempla expresamente que el proceso puede no tener una ampliación de argumentos del oponente (el artículo 2 dice "dentro de los quince (15) días hábiles de vencido el plazo del artículo 1, *y con independencia de que los oponentes hayan ampliado fundamentos o no*, la Dirección Nacional de Marcas notificará al solicitante […]").

La ampliación de fundamentos también permite ofrecer pruebas. De conformidad con el artículo 4 de la Disposición 138, la oportunidad procesal de ofrecer prueba es al momento de la ampliación y no después. Por lo demás una mejor fundamentación va ayudar al INPI a resolver mejor la oposición y a preservar los derechos del oponente frente a una eventual oposición. Incluso podrá ser tenido en cuenta como una actitud positiva por los tribunales en el caso de un recurso directo.

3.2.2. Notificación

Actualmente las notificaciones para mantener la oposición y ampliar fundamentos tienen lugar por medio de la publicación en el Boletín como ocurría con otras notificaciones desde el decreto 1141/2003. Se espera que más adelante, con el expediente y la notificación electrónica funcionando, la notificación sea directa al interesado.

El 31 de octubre de 2018 se publicó el primer Boletín que notificó a los oponentes para que ratificasen sus oposiciones, pagasen la tasa y ampliasen sus fundamentos, dando comienzo al nuevo procedimiento de resolución administrativa de oposiciones. Esa primera notificación contempló a las oposiciones cuyo plazo anual para llegar a un acuerdo entre partes haya vencido entre el 13 de enero de 2018 y el 7 de febrero de 2018, más los trámites en los cuales las partes hayan solicitado expresamente que el INPI resuelva la oposición. Según informó la Asociación Argentina de Agentes de la Propiedad Industrial (AAAPI), se trataría de 1.400 trámites aproximadamente.

3.2.3. Falta de ratificación. Llamado de atención. Efectos

La oposición debe ratificarse o mantenerse mediante el pago de la tasa indicada en el anexo II de la Resolución P-183/2018. La falta de pago transforma la oposición en un llamado de atención. Cabe recordar que el llamado de atención no tiene el efecto de la oposición de bloquear el trámite del registro de marcas como sí lo hace la oposición.

El llamado de atención no obliga al INPI. Pero el INPI le correrá traslado a la contraparte, como es la práctica desde hace un tiempo con los llamados de atención presentados[10]. La contraparte puede no contestar el llamado de atención y ello no trae aparejado ninguna consecuencia. Por ello, el llamado de atención podrá ser o no ser considerado por el INPI.

La falta de pago y la transformación de la oposición en llamado de atención ocurren en forma automática y no requieren de un pronunciamiento expreso del INPI (la norma dice "automáticamente y sin más trámite no se abrirá la instancia administrativa de oposiciones").

Esto impacta en el curso del procedimiento porque no se produce la apertura de la instancia administrativa de oposiciones: el oponente deja de ser tal y no queda legitimado para recurrir el rechazo de la oposición pues, en teoría, no hay procedimiento de oposiciones y la solicitud de marca pasa al estudio de fondo.

[10] El único supuesto donde no se da traslado es cuando el llamado de atención es reiterativo de la oposición.

3.3. Traslado y contestación de las oposiciones

El artículo 2 del Reglamento dispone que "Dentro de los quince (15) días hábiles de vencido el plazo del artículo 1, y con independencia de que los oponentes hayan ampliado fundamentos o no, la Dirección Nacional de Marcas notificará al solicitante de todas las oposiciones que aún permanezcan vigentes y de sus eventuales ampliaciones y se le otorgará un plazo improrrogable de quince (15) días hábiles para que conteste individualmente cada una de ellas ofreciendo en ese acto las pruebas que estime pertinentes".

Este traslado se fundamenta en el derecho de defensa en juicio (artículo 18 de la Constitución Nacional y artículo 1 LNPA). En el punto anterior dijimos que la ampliación de fundamentos y ofrecimiento de prueba del oponente es una suerte de demanda y esta contestación sería una especie de contestación de la demanda.

El solicitante de la marca debe contestar los argumentos que expone el oponente. En general esto implica alegar y probar la falta de confusión, pero también —de acuerdo con el Derecho y las prácticas vigentes— podrán consistir en sostener otras prohibiciones de registro que hayan sido la base de la oposición. Ni el Reglamento ni la reforma de la Ley N.º 27.444 limitaron la posibilidad de plantear oposiciones sólo a motivos relativos o absolutos de rechazo de marca. Seguirá la práctica de poder invocar fundamentos de toda clase en la oposición, incluyendo marcas de hecho, marcas notorias no registradas en el país, nombre comerciales o designación, denominaciones o razones sociales, derechos de autor y obras intelectuales (y sus personajes o títulos), nombres de dominio, denominaciones de origen o indicaciones geográficas, leyes de lealtad comercial o de competencia desleal y un largo etcétera[11].

¿Qué sucede si el solicitante no contesta el traslado de la ampliación de fundamentos? Al respecto, el Reglamento de oposiciones que comentamos guarda silencio. Pero claramente no tiene ninguna consecuencia negativa, pues el espíritu del Reglamento es acelerar el trámite del registro de marca y evitar que la oposición se transforme es un obstáculo

[11] Otamendi, *Derecho de Marcas*, p. 138; Cabanellas y Bertone, *Derecho de Marcas*, t. II, p. 27 y ss.; Mitelman, *Marcas y otros signos distintivos*, t. I, p. 336.

indebido al registro de la marca. Sin embargo, nos parece que el INPI podrá inferir en forma negativa que la falta de respuesta implica admitir hechos o derecho según las circunstancias del caso.

3.4. Etapa probatoria

3.4.1. Aspectos generales

Según dispone el artículo 4 del Reglamento, "las pruebas ofrecidas por ambas partes, serán proveídas en conjunto luego de vencido el plazo del artículo 2". Respecto a la prueba que se debe acompañar, el Reglamento menciona un solo tipo de prueba en su artículo 4: "La prueba documental o instrumental deberá ser acompañada en el mismo acto de ampliar oposición o de contestarla". Respecto a "los restantes medios de prueba ofrecidos", el Reglamento establece lacónicamente que "serán evaluados por la Dirección Nacional de Marcas en cuanto a su procedencia, así como también el plazo y la forma de producirla".

Con la intención de otorgar celeridad al procedimiento se dispone que "no serán admitidas las que fueren manifiestamente improcedentes o superfluas o meramente dilatorias para la resolución de la instancia". Asimismo, para evitar dilaciones, el Reglamento dispone en el mismo artículo 4 que "Las decisiones que se adopten en orden a la admisibilidad o inadmisibilidad (se refiere a la prueba) serán irrecurribles sin perjuicio de su invocación en la instancia judicial, en su caso".

Finalmente, el Reglamento aprobado por la Resolución 183 dispone en su artículo 4 que "el plazo para la producción de la prueba no podrá exceder de cuarenta (40) días hábiles. Dicho plazo es común y comenzará a correr a partir de la notificación de la providencia que al efecto dicte la Dirección Nacional de Marcas".

Quienes litigamos en la justicia sabemos que los cuarenta días son sólo una expresión de deseo. Existen juicios que han estado abiertos a prueba por años. Para evitar esos cuestionamientos, la Resolución dispone que "Al vencimiento del plazo de prueba fijado por la Dirección Nacional de Marcas se tendrá por decaída la prueba no producida por las partes". Nuevamente, si uno piensa que los cuarenta días hábiles son aproximadamente

dos meses, será difícil lograr que una repartición pública o privada contesten un oficio (mucho menos si hay que diligenciar uno reiteratorio) dentro del plazo señalado. Volvemos a lo señalado al comienzo en cuanto a que la prueba documental o instrumental va a ser lo más importante.

Finalmente, cabe señalar que más allá de las limitaciones probatorias que mencionamos previamente, el artículo 4 del decreto reglamentario de la Ley de Marcas dispone que "El interés legítimo podrá acreditarse por cualquier medio de prueba".

3.4.2. Prueba documental y de registros públicos

Una norma muy positiva en el Reglamento es el artículo 4, que dispone que la Dirección Nacional de Marcas podrá efectuar constataciones electrónicas o informáticas de registros públicos, incluyendo los propios, u otras constataciones electrónicas ofrecidas por las partes, que considere pertinentes. Esto implica que las partes no deberán notarizar ni probar con otra clase de prueba los registros públicos de cualquier índole o sitios web cuando quieran probar algo concreto que surja de ellos en determinado momento. Bastará con referenciarlos incluso sin acompañar una copia de estos (por ejemplo, los títulos marcarios tanto locales como extranjeros). Pero se deberá tener cuidado con los registros digitales que se alteran con el tiempo. El resultado de una búsqueda en Internet puede cambiar todos los días, de acuerdo con su fórmula mágica. Un registro público puede actualizarse mes a mes, con lo cual lo que se informa en un momento puede cambiar al momento de resolver (ej., en trámite, concedido o con oposiciones).

Asimismo, la prueba digital es fácilmente alterable. Un sitio web puede estar caído o darse de baja y volver a estar online más adelante. Por ello lo más recomendable en estos casos será acompañar un acta notarial que dé cuenta de lo que se quiere probar.

3.4.3. Otras cuestiones relacionadas a la prueba

En principio el Reglamento no limita ninguna clase de prueba, pero dado lo expeditivo del trámite resulta obvio que ciertas pruebas comple-

jas como las *pericias o informes técnicos* van a tener que ser reemplazadas por el ingenio de las partes, por ejemplo, acompañando un informe que haga las veces de pericia.

Por ejemplo, en vez de producir prueba pericial contable o informática se podrá adjuntar un informe contable certificado por el colegio respectivo, o un informe de un perito informático sobre un tema técnico. Esto, sin embargo, permitirá prueba de los propios registros contables o informáticos pero no los de la contraparte. En este caso, se podrá esgrimir el principio de la carga de la prueba y la imposibilidad de probar algo fuera del control de una de las partes. Si la contraparte está en mejores condiciones de probar un hecho negativo, no le debería alcanzar con negarlo sino que activamente debe demostrar que tal hecho no le es imputable o que las cosas no son como alega la contraparte. Hay que ver cómo el INPI aplicará la doctrina de las cargas probatorias dinámicas, pero en casos como este deberá hacerlo a menos que quiera implementar otros medios probatorios que retrasarán el trámite del proceso.

No debería ser admitida la prueba de *absolución de posiciones*, que como se sabe no sólo no sirve para nada sino que es una pérdida de tiempo. Lo mismo puede decirse del reconocimiento judicial de cosas o hechos, pues el INPI no tiene los recursos para realizar estas verificaciones.

Respecto a la *prueba en el extranjero*, esta tampoco se condice con la celeridad del procedimiento (hay exhortos internacionales que pueden demorar más de dos años de trámite). Por lo tanto la parte deberá aportar los listados correspondientes de marcas, para el caso de intentar probar la notoriedad de su signo, o los casos judiciales que así lo demuestren. Sin perjuicio de ello, el INPI tiene facultades para chequear su propio registro y los registros extranjeros que sean accesibles por Internet. Por lo tanto no será necesario acompañar copias de estas constancias, sino simplemente mencionarlo en los escritos de ampliación de fundamentos o de contestación. Lo mismo ocurrirá con registros públicos nacionales o provinciales.

En cuanto a la prueba testimonial, esta se puede adjuntar en escritos en forma impresa con formato de una declaración jurada del testigo. Su validez y su valoración probatoria dependerán de su correlación con otras constancias del expediente. Lamentablemente el ofrecimiento de testimoniales por vía escrita evita la confrontación del testigo y las repreguntas de la contraparte.

Por lo tanto, si se quiere tener derecho a repreguntar, el INPI podría delegar en los letrados —como hacen varios juzgados comerciales hoy en día— la toma de audiencia en las oficinas de las partes dentro del plazo de prueba.

Otro tema no contemplado en el Reglamento es la prueba de la notoriedad de una marca. En muchos países (Brasil, China, India, Turquía) existe un registro administrativo de marcas notorias, lo cual entendemos que es compatible con el artículo 6 bis del Convenio de París. Las agencias de marcas admiten la inscripción en este registro luego de evaluar sumariamente la notoriedad. La creación por parte del INPI de este registro le facilitaría mucho a esta institución y a las partes la prueba y el reconocimiento de tales signos distintivos sin tener la parte o el INPI que analizar la notoriedad en cada caso cuando esta ya surge de un registro de marcas notorias[12].

A los fines de resguardar el derecho de defensa en juicio, cualquier prueba denegada por el INPI podrá ser replanteada en la alzada, como un agravio concreto dentro del recurso directo. Sin embargo, aventuramos que va a ser difícil que la cámara abra a prueba cada recurso directo. De lo contrario las salas de la Cámara Civil y Comercial Federal terminarían sustanciando todo tipo de pruebas, lo cual no es su función. Una apertura probatoria muy amplia no se condice tampoco con la naturaleza del recurso directo implementado por el artículo 17 de la Ley de Marcas. Sin embargo, la no admisión de las pruebas esenciales para resolver el litigio afectaría la defensa en juicio de los justiciables. Probablemente el estándar para admitir prueba será muy restrictivo, y sólo respecto de aquella prueba que los jueces entiendan era esencial para resolver el litigio y fue injustamente denegada en la instancia administrativa. Por eso los litigantes tendrán que replantear expresamente el pedido de prueba denegada en sede administrativa.

El sistema está ideado para tramitar cada oposición en forma individual. Pero existen casos en los que una misma marca tiene varias oposiciones de terceros y otros en los que un solicitante que presentó la misma marca en varias clases recibe una oposición de la misma marca en cada clase. Con estos casos se van a formar "grupos de casos" y el INPI ha explicado que los van a resolver en forma grupal por el mismo examinador para evitar posibles contradicciones.

[12] Además sería una fuente de ingresos para el INPI.

Dado lo limitado del aspecto probatorio y de su control, existe la posibilidad que una de las partes presente (por error o dolosamente) prueba que no se ajusta a la realidad,[13] y la otra parte no se defienda ni verifique su autenticidad. El INPI, engañado, podría tomar una decisión sobre confundibilidad en base a esta prueba incorrecta. En este caso, entendemos que el fraude demostrado podría ser la base para anular la decisión del INPI. En el caso, la parte perjudicada debería plantear el recurso de revisión del artículo 22 de la LNPA, que es similar a la revisión del Código Procesal Penal que permite abrir una causa fenecida.

3.5. Caducidad o nulidad judicial como defensa en una oposición

El artículo 5 del Reglamento dispone: "En caso de que alguna de las partes plantease la caducidad o nulidad judicial de alguna marca relacionada con el conflicto, las partes deberán tramitar ello ante la justicia competente por la vía que corresponda hasta tanto el INPI reglamente el procedimiento para resolver las caducidades de registro contempladas en el artículo 26 de la Ley N.º 22.362 y nulidades contempladas en el inciso 'a' del artículo 24 del mismo cuerpo legal, sin perjuicio de lo cual la Dirección Nacional de Marcas igualmente resolverá respecto de la confundibilidad de los signos enfrentados y/o de los otros fundamentos de las oposiciones sobre los que pueda expedirse y reservará el expediente para decidir respecto de la concesión del signo una vez resuelta la caducidad o nulidad interpuesta ante la justicia".

Esta norma se refiere a la caducidad o nulidad judicial como defensa en el procedimiento de oposiciones (la norma dice "de alguna marca relacionada con el conflicto"). Con frecuencia, quien enfrenta una oposición puede o bien cuestionar la falta de confusión o atacar la marca del oponente por falta de uso (caducidad) o porque la marca del oponente es nula.

El artículo 5 del Reglamento pospone sin límite temporal claro la posibilidad de plantear caducidad o nulidad bajo la nueva ley. Con anterioridad, bajo el régimen de la Ley N.º 22.362, las partes tenían el derecho y la libertad de plantear estas acciones en sede judicial. La Ley N.º

[13] Ya ha pasado con algunos agentes de la propiedad industrial en respecto a la prueba del uso de la marca, tanto en mediaciones como en sede judicial en juicios de caducidades por falta de uso.

27.444 confinó al litigante a la sede administrativa del INPI. Pero el propio INPI, unos meses más tarde, mediante el artículo 5 del Reglamento que comentamos, dispuso que no será posible resolver la caducidad o nulidad hasta tanto se reglamente el procedimiento y que por lo tanto se debe recurrir a la vía judicial (la norma dice "las partes deberán tramitar ello ante la *justicia* competente por la vía que corresponda").

El artículo 15.5 del Acuerdo TRIPs (Ley N.º 24.425) dispone que "Los miembros publicarán cada marca de fábrica o de comercio antes de su registro o sin demora después de él, y ofrecerán una *oportunidad razonable de pedir la anulación del registro*". Esta norma cubre cancelación de la marca por diversos motivos, incluyendo falta de uso por un plazo determinado.

Por su parte, el artículo 41.2 del Acuerdo TRIPs dispone: "Los procedimientos relativos a la observancia de los derechos de propiedad intelectual serán justos y equitativos. *No serán innecesariamente complicados o gravosos, ni comportarán plazos injustificables o retrasos innecesarios*".

La reforma de la Ley N.º 27.444 atribuyó la resolución de nulidades y caducidades al INPI. Por lo tanto, ahora sólo el INPI, y no la justicia, es competente para resolverlas. El Reglamento —por su rango normativo— no puede modificar la Ley N.º 27.444. El INPI no ha reglamentado por ahora el procedimiento para resolver las nulidades pues está abocado a resolver la cuestión relacionada con las oposiciones. Sin embargo, la falta de reglamentación impide a quienes tienen algún interés legítimo la posibilidad de cancelar una marca (ya sea por falta de uso o por infracción a la Ley de Marcas), con lo cual si esta ausencia de reglamentación se prolonga en el tiempo, nos encontraríamos ante una violación del artículo 15.5 del Acuerdo TRIPs por parte del Estado argentino. Esta violación consiste en no ofrecer al litigante una "oportunidad razonable de pedir la anulación del registro" conforme exige el artículo 15.5 del Acuerdo TRIPs.

3.6. Argumentos finales

El artículo 6 de la Resolución 138 dispone que "producidas las pruebas o vencido el plazo para ello, y previo a que la Dirección Nacional de Marcas se expida sobre la procedencia de la oposición, si no hubiese ninguna cuestión previa de procedimiento a resolver, se notificará a las partes por el plazo

común de diez (10) días hábiles para que presenten un escrito, con carácter voluntario, con los argumentos finales que deseen manifestar". Lo que en el litigio judicial de cese de oposición era un alegato, en el procedimiento administrativo de resolución de oposiciones recibe el nombre de "escrito, con carácter voluntario, con los argumentos finales que deseen manifestar".

El alegato siempre versó sobre la valoración de la prueba, pero este escrito voluntario parece ser una forma de reafirmar los argumentos de las partes. No debe versar sólo sobre la prueba sino sobre los argumentos finales que deseen manifestar las partes. Es una suerte de escrito de cierre de procedimiento. En algunos casos será importante, en otros será sobreabundante.

3.7. Métodos alternativos de resolución de conflictos

Un dato positivo del Reglamento es el fomento de los métodos alternativos de resolución de disputas tales como la mediación o la conciliación. Así, el segundo párrafo del artículo 6 del Reglamento dispone que "Dentro de dicho plazo las partes podrán informar que han iniciado un procedimiento de mediación o conciliación u otro método alternativo de resolución de conflictos, acreditando debidamente dicho extremo. Ese informe deberá ser efectuado en un escrito en conjunto. En tal caso, se producirá por única vez la interrupción automática del plazo del primer párrafo para ambas partes por el término improrrogable de treinta (30) días hábiles; contado desde la presentación del escrito respectivo".

La norma requiere un escrito conjunto, lo que implica que ambas partes deben estar de acuerdo en suspender el procedimiento administrativo cuya característica es la celeridad. No es posible solicitar una mediación en forma unilateral. A nuestro modo de ver, esta posibilidad está mal ubicada, sólo al final del procedimiento antes de la resolución. De hecho, las partes en cualquier momento y de común acuerdo pueden recurrir a un método alternativo de resolución de disputas y no sólo en esta instancia, pero en ese caso no parece tener el efecto de suspender el procedimiento.

En materia de signos distintivos la mediación ha demostrado ser una excelente herramienta para resolver disputas de confusión marcaria. Durante años entre el 60% y 70% de las oposiciones se resolvían en la instancia de mediación y así se evitaban largos pleitos. En el Derecho Comparado,

algunos países lo han instaurado en el ámbito administrativo como opción, por ejemplo en Brasil,[14] Singapur[15] y más recientemente en Polonia[16].

La norma dispone que "Dentro de este último plazo las partes deberán concluir la mediación, conciliación o el método alternativo de resolución de conflictos que hubieren manifestado haber iniciado. Vencido el mismo, automáticamente, comenzará un nuevo plazo común de diez (10) días hábiles con el mismo efecto y alcance del que había sido interrumpido. En caso de que las partes solucionen en el conflicto en el procedimiento elegido, deberán informarlo a la Dirección Nacional de Marcas antes de que venzan los plazos, acompañando las constancias de ello. En tal supuesto, se tornará abstracto el resolver sobre dicha solución, más los términos de la misma no obligarán a aquella en la resolución respecto de la concesión de la marca".

El acuerdo de partes se puede presentar en cualquier momento, esto es, al comienzo de procedimiento, en medio del trámite o antes de la decisión del INPI. La resolución lo señala en este punto pues es la última oportunidad donde las partes pueden acordar y ahorrarle al INPI el estudio del expediente, pero nada impide que ocurra antes.

Respecto al arbitraje, el Reglamento no lo menciona. Sin embargo, entendemos que este se presenta como una alternativa ideal a la resolución de oposiciones por el INPI. La decisión acerca de si una marca es confundible con otra o si una oposición está fundada es materia arbitrable porque no está prohibida por el artículo 1651 del Código Civil y Comercial de la Nación. En tanto el acuerdo de arbitraje se limite a prohibiciones relativas de registro,[17] no vemos problema para que el INPI, mediante una reglamentación apropiada, establezca la posibilidad de someter a arbitraje dicha controversia. Esto le permitiría ahorrarse el trabajo de estudiar y resolver la oposición dejando que lo hagan las partes mediante la elección de un tercero (el árbitro). La lógica de las prohibiciones relativas —según el nuevo artículo 47 de la LM— es que no involucran una cuestión de orden público y las partes (o un árbitro

[14] Ver WIPO Mediation for Proceedings Instituted in the Brazilian National Institute of Industrial Property (INPI-BR), http://bit.ly/2KvJ8jd

[15] Ver: http://bit.ly/2H4irA7

[16] Ver WIPO Mediation for Proceedings Instituted in the Patent Office of the Republic of Poland (PPO), http://bit.ly/2TtmvyC

[17] Las prohibiciones absolutas serán resueltas por el INPI al decidir la concesión o no de la marca.

elegido por ellas) pueden acordar en forma definitiva sobre ellas.

En tal sentido sería posible implementar el arbitraje para resolver oposiciones. El INPI, al momento de intimar a mantener la oposición, ampliar y contestar la demanda, puede otorgar a las partes la posibilidad de que ambas pacten que la cuestión planteada en la oposición será resuelta por un árbitro especialista en marcas en vez de seguir el procedimiento reglamentado por el INPI. Este procedimiento de arbitraje podría ser administrado por una institución reconocida (como la AAAPI, Cámara de Agentes de la Propiedad Industrial de la Républica Argentina —CAPIRA— y la Organización Mundial de la Propiedad Intelectual —OMPI—, o por alguna de ellas a elección de las partes) creando una suerte de arbitraje institucional. El arbitraje podría tener su propio reglamento o bien aplicar subsidiariamente las reglas del CCCN (artículo 1650 y ss.) o incluso de la Ley de Arbitraje Comercial Internacional para el caso que las partes sean extranjeras. Finalmente, una vez adoptada, la decisión del árbitro es comunicada al INPI quien la implementa de acuerdo con el Reglamento.

La adopción de este sistema requerirá cierta madurez y visión moderna y práctica sobre los métodos alternativos de solución de disputas por parte de todos los operadores jurídicos involucrados.

El decreto reglamentario de la Ley de Marcas dispuso en su artículo 16 lo siguiente: "Dentro del plazo de TRES (3) meses previsto en el presente artículo, solicitante y oponente u oponentes podrán recurrir a cualquier método alternativo de resolución de conflictos con la finalidad de arribar a un acuerdo sobre el levantamiento parcial o el retiro de la oposición. La Autoridad de Aplicación podrá dictar la normativa complementaria y/o aclaratoria que resulte necesaria a los fines del procedimiento para la resolución de las oposiciones en sede administrativa. La decisión que recaiga se limitará a resolver únicamente si la oposición u oposiciones que se mantengan vigentes son fundadas o infundadas".

3.8. Resolución de la Dirección Nacional de Marcas

Si las partes no ofrecen evidencia porque la cuestión se puede resolver sin prueba, simplemente cotejando los registros en pugna, entonces el INPI pasará a resolver directamente la cuestión.

Si existió prueba, el artículo 9 del Reglamento dispone que una vez vencido el plazo del artículo 6 (los cuarenta días hábiles), si la cuestión no se hubiese declarado abstracta previamente, la Dirección Nacional de Marcas resolverá respecto de si las oposiciones que permanezcan vigentes contra la solicitud son fundadas o infundadas. Esta es la decisión que pone fin al procedimiento administrativo de resolución de disputas. Contra dicha decisión podrá apelar el oponente o el solicitante según el caso.

En cuanto a la forma que deberán adoptar las decisiones, recordamos que el artículo 41.3 del Acuerdo TRIPs dispone: "Las decisiones sobre el fondo de un caso se formularán, preferentemente, por escrito y serán razonadas. Se pondrán a disposición, al menos de las partes en el procedimiento, sin retrasos indebidos. Sólo se basarán en pruebas acerca de las cuales se haya dado a las partes la oportunidad de ser oídas".

Dada la importancia que van a tener los criterios que adopte el INPI en cada caso, será importante que estas decisiones se publiquen y sean accesibles a los agentes de propiedad industrial. De esta forma estos podrán conocer los criterios que el INPI adoptará en cada caso tanto en temas de fondo como procedimentales del Reglamento.

3.9. Recurso directo de apelación

3.9.1. Introducción

El artículo 17 segundo párrafo de la LM dispone que "Las resoluciones por oposiciones que dicte la Dirección Nacional de Marcas serán sólo susceptibles de recurso directo de apelación ante la Cámara Nacional de Apelaciones en lo Civil y Comercial Federal dentro de los treinta (30) días hábiles de su notificación. El recurso deberá presentarse en el Instituto Nacional de la Propiedad Industrial, quien lo remitirá a la justicia en las condiciones que fije la reglamentación".

El artículo 10 del Reglamento dispone que "contra la resolución final que dicte la Dirección Nacional de Marcas en la instancia administrativa de resolución de oposiciones se podrá interponer únicamente recurso directo de apelación previsto en el artículo 17 de la Ley N.º 22.362, y su

presentación deberá cumplir con las formalidades previstas por el Código Procesal Civil y Comercial de la Nación y concordantes, que resulten aplicables".

Este recurso directo es necesario por lo dispuesto en el artículo 41.4 del Acuerdo TRIPs que dispone: "Se dará a las partes en el procedimiento la oportunidad de una revisión por una autoridad judicial de las decisiones administrativas finales y, con sujeción a las disposiciones en materia de competencia jurisdiccional previstas en la legislación de cada Miembro relativa a la importancia de un caso, de al menos los aspectos jurídicos de las decisiones judiciales iniciales sobre el fondo del caso". La norma es clara que por lo menos debe ser posible revisar los aspectos jurídicos del caso.

3.9.2. Requisitos formales

El Reglamento dice escuetamente que "su presentación deberá cumplir con las formalidades previstas por el Código Procesal Civil y Comercial de la Nación (CPCC) y concordantes, que resulten aplicables". Lo mismo establece el decreto reglamentario de la ley de marcas en su artículo 17 al repetir que "la presentación de este recurso deberá cumplir con las formalidades previstas por el Código Procesal Civil y Comercial de la Nación y concordantes".

La remisión parece difícil de interpretar porque el CPCC no contiene formalidades sobre un recurso directo y a escala nacional se carece de un código en lo contencioso administrativo que establezca los recaudos generales de dicha clases de medios impugnativos.

Sin embargo, la doctrina administrativa interpreta que un recurso directo equivale a una acción judicial[18]. Se señala que los recursos directos

[18] Al respecto se ha dicho que "los llamados recursos directos para ante distintas Cámaras de Apelaciones que diversas leyes prevén para la revisión judicial de los actos administrativos, incluidos aquéllos que revisten naturaleza materialmente jurisdiccional, no constituyen recursos procesales, sino acciones judiciales de impugnación de instancia única, para cuya sustanciación, salvo disposición expresa en contrario de la pertinente ley que lo instituye, resultan aplicables las normas que regulan el procedimiento judicial de esta". Cfr. Biotti, María Alejandra, "Algunas precisiones sobre los recursos directos en el contencioso", en la obra colectiva *Una mirada desde el fuero contencioso administrativo federal sobre el derecho procesal administrativo*, Marcelo A. Bruno dos Santos (dir.), 1.ª edición, Buenos Aires, FDA, 2012, con cita de CNFed. CA, Sala I, 2/XI/00,

son modos autónomos de impugnación de actos administrativos, por lo que, por su naturaleza, constituyen acciones judiciales. Es decir, los recursos directos no son sino acciones procesales de un tipo especial que se inician generalmente por ante segunda instancia. Y por eso se remiten a las reglas del proceso civil y comercial,[19] tal como hace el Reglamento en el artículo 10. Entendemos entonces que se deberán aplicar los requisitos del artículo 330 del CPCC porque es la primera intervención judicial del caso motivada por la oposición que fue aceptada o rechazada por el INPI.

Siguiendo el artículo 330 del CPCC, el recurso directo deberá contener por lo menos: 1) el nombre y domicilio del demandante; 2) el nombre y domicilio del demandado; 3) la cosa demandada: en el caso que se declare fundada o infundada la oposición marcaria; 4) los hechos en que se funde, explicados claramente; 5) el derecho expuesto sucintamente, evitando repeticiones innecesarias; 6) la petición en términos claros y positivos (en este caso que las marcas solicitadas son o no son confundibles con las del oponente).

En el recurso directo, el recurrente debe atacar los argumentos de la otra parte, pero también deberá criticar el acto administrativo que decide en contra de su la pretensión. Las partes en el procedimiento de oposiciones son el solicitante de la marca y el oponente; el INPI no es parte. Si el INPI fuera parte, no serían facultades jurisdiccionales sino la función administrativa lo que se ataca. La apelación mediante un recurso directo que debe resolver la Cámara de Apelaciones es un conflicto entre privados regido por el Derecho privado que por una razón de eficiencia resuelve primero un órgano de la administración especializado como es la Dirección Nacional de Marcas del INPI[20].

Leconte, Ricardo H. c/ BCRA resol. 155/00.

[19] González Arzac, Rafael M., "Legitimación procesal de los órganos administrativos en los recursos judiciales contra sus decisiones", con cita en Linares, Juan F., "El caso administrativo no previsto y la analogía jurídica en la jurisprudencia de la Corte Suprema de Justicia de la Nación", *LL*, 24-178; Marienhoff, Miguel, *Tratado de Derecho Administrativo*, Buenos Aires, Abeledo-Perrot, 1965, pp. 172 y 268; Fiorini, Bartolomé A., *Manual de Derecho Administrativo*, Buenos Aires, La Ley, 1968, p. 93.

[20] A futuro, con el fin de lograr mayor especialización, lo más práctico sería que se cree un tribunal administrativo especializado en temas marcarios (como sucede en Estados Unidos con el Trademark Trial & Appeal Board, TTAB) que funcione como alzada administrativa de la Dirección Nacional de Marcas y que la revisión judicial sea excepcional dada la especialización de este tribunal.

Con este recurso, deberá acompañarse el pago de la tasa administrativa para el recurso directo. Esta tasa es de 850 pesos, según el anexo II de la Resolución P318/2018. El no pago de la tasa implica que INPI no remitirá el expediente junto con el recurso a la cámara. Pero tampoco implica el rechazo automático del recurso. Esto deberá tener lugar sólo con previa intimación a abonar la tasa dentro del plazo legal. Lo contrario implicaría privar de la vía judicial al apelante sin respetar el debido proceso legal (artículo 18 de la Constitución Nacional).

El recurso directo se interpone ante el INPI (artículo 17 LM). Está dispuesto así por una cuestión práctica: el INPI debe tomar nota de qué marcas solicitadas aún tienen pendiente una decisión judicial, y cuáles deben seguir el trámite administrativo posterior. Parece sobreabundante decirlo, pero señalamos que el recurso directo del artículo 17 de la LM excluye la revisión del acto judicial por la LNPA o la demanda contenciosa. La interposición de una demanda ante instancias inferiores (u otro fuero) sustraería a la cámara la competencia que la Ley N.º 27.444 le atribuye en forma directa a ella.

Una vez interpuesto el recurso directo ante el INPI, lo único que este puede hacer es recibir el recurso y elevarlo a la cámara. En tal sentido, el artículo 10 del Reglamento dispone que "Dentro de los diez (10) días hábiles el INPI remitirá el recurso interpuesto junto con copia de las actuaciones relacionadas a la oposición respectiva, a la Cámara Nacional de Apelaciones en lo Civil y Comercial Federal de la Capital Federal, para que dicha instancia judicial resuelva la contienda trabada entre solicitante y oponente".

Con este recurso directo comienza el trámite judicial de las oposiciones. A partir de la interposición del recurso, se aplican las normas del CPCC en cuanto a las formalidades del mismo, y le compete a la justicia —no al INPI— valorar las formalidades procesales del recurso directo. Si el escrito tiene firma o no de abogado (necesario por ser un recurso judicial), si está fundado, si fue interpuesto dentro de los treinta días de plazo, o si menciona apropiadamente las marcas u oposiciones correctas es algo ajeno al INPI: el trabajo del INPI termina con su decisión[21].

[21] Es frecuente que que muchas veces los órganos administrativos se extralimitan y quieren hacer un control de procedencia del recurso. La jurisprudencia del fuero Contencioso Administrativo Federal es clara en ese sentido y la sede administrativa no tiene control sobre el recurso: se tiene

Igualmente, entendemos que si bien el INPI no es juez del recurso (pues es un recurso directo), deberá por lo menos verificar qué se está apelando y cuáles oposiciones están involucradas, para certificar si otras marcas quedaron libres de oposición y de recurso y seguir con su trámite. Si no cumple con su obligación de elevar el expediente, el recurrente podrá ir en queja a la cámara.

Este recurso directo no requiere mediación previa. Si bien la mediación en Argentina es prejudicial, esta se refiere al inicio de acciones legales, lo que no incluye un recurso directo contra una resolución del INPI. Siempre queda la posibilidad de que el juez de la causa, invocando la disposición vigente en la Argentina (artículo 16 inciso "d" Ley N.º 26.589) convoque a las partes a una mediación.

3.9.3. Naturaleza del recurso

Cabe preguntarse por la naturaleza de esta apelación contra la decisión de oposiciones. ¿Se apela contra el Estado, o contra la oposición que es declarada infundada o fundada? El artículo 10 del Reglamento es claro en este sentido cuando dice que la justicia debe resolver "la contienda trabada entre solicitante y oponente". Es decir, se trata de un conflicto entre dos particulares respecto a la confusión de una marca. En este sentido no cambia el concepto que existía bajo el texto original de Ley N.º 22.362 antes de su reforma por la Ley N.º 27.444. Pero al establecerse un recurso directo, se ha creado una revisión judicial *sui generis*. Bajo la Ley N.º 22.362 la cuestión se sometía directamente a la justicia federal de primera instancia con la posibilidad de revisar esa decisión en cámara; ahora, en cambio, se somete directamente a la cámara de apelaciones, con una decisión previa de la Dirección Nacional de Marcas del INPI.

Al respecto Mitelman,[22] quien comentó en su momento el régimen del Decreto 27/2018 —de contenido similar a la Ley N.º 27.444—, sostuvo lo siguiente:

que limitar a elevarlo al tribunal competente para que lo resuelva.

[22] Mitelman, "Efectos del Decreto N.º 27/2018 en la legislación de marcas y modelos industriales", *elDial*, 25 de abril de 2018.

¿Contra quién debe interponerse el recurso de apelación? ¿Contra la autoridad de aplicación que ha dictado la resolución? ¿O contra el solicitante u oponente que ha sido favorecido? Nos inclinamos por la segunda opción.

La oposición es un acto voluntario emanado de un particular. Practicada la publicación de la solicitud de registro en el Boletín de Marcas, ningún sujeto tiene la carga u obligación de formular oposición. Se puede válidamente decidir no hacerlo y aguardar a que la autoridad de aplicación dictamine acerca de la registrabilidad de la marca pretendida. Si se ejerce la opción de deducir oposición, sigue rigiendo el artículo 4 LM que requiere "interés legítimo" del oponente. Si su retiro vía negociación deviene infructuoso, entonces la Dirección Nacional de Marcas es llamada a resolver. Se desprende entonces que el ente administrativo no participa de oficio, sino que su intervención es convocada por una disposición legal ante la actuación de dos sujetos (solicitante y oponente) que no lograron previamente solucionar sus diferencias.

Está claro que la resolución proviene de la autoridad estatal, pero ella no ha intervenido por iniciativa propia, sino ante la controversia suscitada entre dos particulares, y ha dictaminado a favor de uno y en detrimento de otro se supone en base a los fundamentos y prueba ofrecidas por las partes. En este escenario la apelación debería ser planteada por el sujeto perdidoso contra aquél que se ha beneficiado del dictamen favorable.

Diferente es la situación si en ausencia de oposición, al evaluar las condiciones de registrabilidad la entidad estatal deniega el registro invocando, por ejemplo, la similitud con otra marca previamente inscripta. En esta hipótesis, la iniciativa de invocar semejante antecedente proviene del INPI y la acción debe ser formulada contra el ente, siendo aplicable el artículo 21 (cfr. Decreto N.º 27/2018).

3.9.4. Tramo judicial del recurso directo

¿Cómo se desarrollará esta recurso en la Cámara de Apelaciones? Es de esperar que luego de recibido el recurso directo la oficina de sorteos

de la cámara asignará una sala que estudiará el recurso y la presencia de todos los requisitos necesarios. La sala deberá hacer saber a las partes los jueces que van a entender en el recurso, para eventuales recusaciones. Una vez firme esta providencia, se ordenará correr traslado a la contraparte (artículo 338 CPCC). Este traslado, que como vimos ocurre en sede judicial y no administrativa, es a los fines de que la parte apelada ejerza su derecho de defensa. Por otra parte, si el recurso directo puede ser entendido como una demanda judicial, su contestación se equipara a una contestación de demanda.

La contestación debe cumplir con el artículo 356 del CPCC. Versará sobre los requisitos formales del recurso directo, pero también sobre el fondo del asunto. Se podrá ofrecer nueva prueba documental para contradecir la del recurrente, y también toda otra clase de prueba admitida por el CPCC.

La amplitud probatoria para ambas partes es importante porque la que se podrá ofrecer en sede administrativa es muy escueta según el Reglamento. Asimismo, de la nueva prueba se deberá dar traslado al recurrente (artículo 358 CPCC).

3.10. Concesión o denegatoria de la solicitud de marca

El artículo 11 del Reglamento dispone que "encontrándose firme o consentida la resolución de la oposición, la Dirección Nacional de Marcas, si estuviese en condiciones de hacerlo, resolverá seguidamente y por medio de otro acto administrativo, respecto de la concesión o de la denegatoria de la solicitud de marca. Por tal motivo, la acción de denegatoria de marca no procederá contra aquellas resoluciones basadas exclusivamente en oposiciones fundadas".

¿Por qué se separa la decisión de la oposición del de la concesión? Se tratan de dos cuestiones muy diferentes entre sí. En la primera, se debe decidir si la oposición es o no es fundada. Y debe existir la posibilidad de las partes de apelar esta decisión. La segunda es más una decisión propia del poder de policía del INPI en materia de marcas. Esta es una razón más para insistir en que el INPI implemente en la práctica la facultad que tiene de "limitar el examen de las solicitudes a las prohibiciones absolutas

o que se relacionen con el orden público, supeditando las relativas a su planteamiento por terceros", conforme lo autoriza el artículo 47 de la LM. Numerosas leyes y prácticas del derecho comparado han implementado esta forma de analizar las marcas[23].

En síntesis, el oponente que no mantiene la oposición no es parte. Además al no mantener la oposición no se produce la apertura del procedimiento de oposiciones y el INPI no resuelve si la oposición es o no fundada, sino que sólo la tendrá en cuenta como llamado de atención. No hay entonces nada que resolver, y por ende, nada para apelar.

Como no es parte, el *pretenso* oponente no debería poder recurrir la decisión adversa de concesión alegando fundamentos vertidos en la oposición que no mantuvo mediante el pago de la tasa en sede administrativa. Ello explica la frase final del artículo 11 del Reglamento que dispone: "Por tal motivo, la acción de denegatoria de marca no procederá contra aquellas resoluciones basadas exclusivamente en oposiciones fundadas".

4. Conclusiones

La reforma de la Ley N.º 27.444 y el Reglamento de Oposiciones que comentamos en esta nota es algo positivo para el sistema marcario argentino. Si el resultado va a ser que las oposiciones no se transformen en muchos casos en obstáculos irrazonables e insalvables, la reforma y su implementación habrán valido la pena. La implementación sin embargo está siendo difícil por la coyuntura actual.

La Resolución 183/2018, como se señaló, era muy esperada, dado que el cambio de reglamentación para el sistema de oposiciones generó mucha expectativa en los agentes de propiedad industrial acerca de cómo funcionará este nuevo procedimiento y cuáles serían sus rasgos esenciales. La idea de resolver oposiciones en el ámbito administrativo con una apelación judicial ante la Cámara Civil y Comercial Federal puede ser muy positiva para destrabar el trámite de registros de marca y evitar que estos duren años.

[23] Ver MPI, *Study on the Overall Functioning of the European Trademark System*, p. 18. Todos los países de la UE analizan de oficio las prohibiciones absolutas. De los 28 miembros de la UE, sólo 12 analizan también las relativas. El resto no lo hace y lo deja supeditado al interés de los particulares.

Pero esta reforma debe ir acompañada por un cambio de mentalidad de los operadores del sistema en muchos otros conceptos. El Derecho Marcario argentino tiene que evolucionar hacia conceptos más universales e internacionales. A modo de ejemplo, señalamos la extensión o alcance del concepto de confusión marcaria al evaluar presentar una oposición. También se requieren reglas más claras para que se diferencien las prohibiciones absolutas de las relativas en materia de registro de marca (dejando las relativas a la negociación y decisión de las partes). Incluso habría que evaluar la instauración de un procedimiento arbitral de resolución de disputas en la sede del INPI para tercerizar las decisiones sobre confusión marcaria usando a los propios agentes de propiedad industrial y con la ayuda de las asociaciones de agentes existentes u organizaciones internacionales. Todo esto el INPI lo puede hacer a través de las disposiciones que quedó autorizado a realizar en virtud de la reforma del artículo 47 de la Ley de Marcas.

Algunos comentarios sobre la Resolución N.º 1378/2019 de la Secretaría de Gobierno de Modernización dependiente de la Jefatura de Gabinete de Ministros, relativa a la aplicación de la Sanción de Caducidad de Licencia de Firma Digital a un certificador licenciado dentro de la Infraestructura de Firma Digital de la República Argentina (IFD-RA)

por Leonor Guini

El ente licenciante conformado por el Ministerio de Modernización como autoridad de aplicación de la Infraestructura de Firma Digital de la República Argentina (IFD-RA) y la Secretaría de Gobierno de Modernización interviene en el otorgamiento de licencias a los certificadores, define la existencia de una Autoridad Certificante Raíz Nacional para la emisión de los certificados a los certificadores licenciados y, conforme surge del artículo 40 de la Ley N.º 25.506, interviene en la aplicación de sanciones a los certificadores licenciados ante el incumplimiento de sus obligaciones.

En el presente caso, la sanción impuesta a Encode S. A. en su carácter de certificador licenciado es la más grave que establece la normativa y se trata de la "caducidad de licencia", sanción establecida en el artículo 44 de la Ley N.º 25.506, la que constituye asimismo una de las causales de cese de la actividad del certificador dispuesta por el ente licenciante (artículo 22 de la Ley N.º 25.506).

Se deja constancia de que en la actualidad los efectos de la medida impuesta se encuentran suspendidos temporariamente conforme se explicará a continuación.

1. Cuándo procede

Todos los certificadores licenciados están sujetos a un régimen de auditoría previa, llamada también "auditoría de conformidad", que es la que les habilita la aprobación del proceso de licenciamiento y

la obtención de la calidad de certificadores licenciados dentro de la IFD-RA.

Esta auditoría previa tiene como objeto mínimo evaluar la confidencialidad y la calidad de los sistemas utilizados, la integridad, confidencialidad y disponibilidad de los datos, así como también el cumplimiento de las especificaciones del Manual de Procedimientos, de la política de seguridad y del plan de contingencia aprobados por el ente licenciante.

Conforme surge de los artículos 53 a 55 de la Resolución N.º 399/16, existen revisiones post-licenciamiento, por lo que los certificadores licenciados están sujetos a auditorías anuales, u ordinarias, y a inspecciones extraordinarias[1].

Cuando de dichos procesos de auditoría surgen graves irregularidades que infringen el marco normativo de firma digital de la República Argentina, el ente licenciante está habilitado para aplicar alguna de las sanciones establecidas en el título X de la Ley N.º 25.506 en sus artículos 40 a 46, previa instrucción sumarial.

En el caso en examen, el ente licenciante decidió aplicar la máxima sanción que puede aplicarse a un certificador licenciado: la sanción de "caducidad de licencia", establecida en el artículo 44 de la Ley N.º 25.506, sanción que, una vez firme, inhabilita a su titular y a los integrantes de sus órganos directivos por el término de diez años para ser titular de licencias.

La sanción interpuesta por la Resolución N.º 1378/19, del 15 de agosto de 2019, de la Secretaría de Gobierno de Modernización fue recurrida por el certificador y se encontraron suspendidos sus efectos hasta tanto se agote la vía administrativa a través de la Resolución del Recurso Jerárquico o hasta que se cumpla el plazo máximo establecido por el artículo 5 de la Ley N.º 26.854.

---

[1] Conforme surge de la Resolución N.º 399/16, la Sindicatura General de la Nación realizará las auditorías previstas en el capítulo VII de la Ley N.º 25.506. Los dictámenes y demás documentación vinculada que surjan de las auditorías deberán ser remitidos en copia autenticada a la Secretaría de Modernización Administrativa del Ministerio de Modernización.

Artículo 55. La Secretaría de Modernización Administrativa del Ministerio de Modernización, a su cargo, podrá realizar u ordenar inspecciones extraordinarias, de oficio o en caso de denuncias de terceros fundadas en presuntas deficiencias o incumplimientos incurridos por el certificador licenciado.

2. El caso concreto. Antecedentes

Que con fecha 1 de marzo de 2017 se procedió a notificar a Encode S. A. el procedimiento de auditoría anual ordinaria por parte de la Sindicatura General de la Nación en su carácter de ente auditante, como asimismo, los puntos de control sobre los que versaría dicha auditoria.

Se deja constancia de que uno de los puntos de control más importantes de toda auditoría consiste en comprobar cómo el certificador licenciado lleva a cabo el proceso de emisión de certificados y si cumple con todas las condiciones de seguridad establecidas en el marco normativo de firma digital de la República Argentina.

Del informe final no surgen fallas significativas en cuanto al cumplimiento de las exigencias tecnológicas y de seguridad física y lógica, así como de los procedimientos aprobados por la autoridad de aplicación en el momento del licenciamiento de la empresa, pero sí ha dejado en evidencia *modificaciones significativas* de aspectos que fueron objeto de revisión al momento del otorgamiento de la licencia.

Del informe de auditoría surge específicamente que el auditado había procedido a denunciar el reemplazo del dispositivo del sitio de contingencia luego de haber transcurrido nueve meses de haberlo llevado a cabo, conducta que resulta violatoria de lo dispuesto en la Ley N.º 25.506, artículo 21, inciso *q*, y el artículo 55 de la DA 927/2014 (reemplazado por el artículo 50 de la Resolución MM N.º 399-E/16).

Se deja constancia de que todos los artículos referidos aluden a la obligación que asume todo certificador de informar en forma inmediata al ente licenciante sobre cualquier cambio en los datos relativos a su licencia.

El artículo 50 de la Resolución N.º 399/16 específicamente considera que cualquier modificación sobre aspectos significativos que fueron objeto de revisión al momento de otorgamiento de la licencia, debe ser denunciado inmediatamente a los efectos de su aceptación o rechazo por la Secretaría de Modernización.

Por otro lado, la auditoría también detectó el incumplimiento de lo determinado por el Anexo I Apartado VII de la Resolución N.º 399/16 respecto al ciclo de vida de las claves criptográficas utilizadas por el certificador.

Respecto de los Oficiales de Registro de la AC de Encode S. A., se detectó que se encontraban utilizando dispositivos criptográficos inferiores a los estándares definidos por la autoridad de aplicación, lo que implica una falta grave que vulnera lo determinado en el artículo 21 incisos *d* y *v* de la Ley N.º 25.506, y los artículos 19 inciso *3* y 28 inciso *9* del Anexo al Decreto N.º 182/19.

Se debe resaltar que toda autoridad de registro tiene que utilizar dispositivos criptográficos con certificación *overall* FIPS 140 (versión 2) nivel 2 o superior, ya que son un elemento clave en el proceso de emisión de los certificados digitales a los particulares, y las firmas digitales se deben generar en un ambiente seguro que garantice la confiabilidad de los sistemas de acuerdo con los estándares aprobados por la autoridad de aplicación.

A todo lo detectado dentro del proceso de auditoría anual ordinaria anteriormente referido se agrega la denuncia efectuada por terceros contra el certificador en cuestión, por lo que se procedió a ampliar la auditoría y a iniciar el correspondiente expediente penal.

El organismo auditante concluye confirmando que la gestión de las claves criptográficas de los suscriptores y su almacenamiento era generada por software y administrada por una plataforma centralizada perteneciente a Encode S. A., infringiendo de este modo lo dispuesto por la Resolución de la Secretaria de Modernización N.º 63/18.

Atento a lo expuesto, la Secretaría de Gobierno de Modernización procede al dictado de la Resolución N.º 1378/19 del 15 de agosto de 2019 de la Secretaría de Gobierno de Modernización, por la cual se aplica la sanción de caducidad de licencia antes mencionada.

Dicha medida fue recurrida mediante otra medida cautelar urgente iniciada contra el Estado nacional y la Secretaría de Gobierno de Modernización a los fines de obtener la suspensión de los efectos de la sanción de caducidad impuesta al certificador.

El Juzgado de Primera Instancia en lo Contencioso Administrativo N.º 10 ante el cual tramitó la referida cautelar, dispuso la suspensión de los efectos de la medida decretada hasta que se agote la vía administrativa a través de la Resolución del Recurso Jerárquico o hasta que se cumpla el plazo máximo establecido en el artículo 5 de la Ley N.º 26.854.

El juez llega a tal conclusión valorando las siguientes circunstancias: las pruebas aportadas en la causa penal por el certificador, el hecho de no haberse instruido por parte del ente licenciante el sumario correspondiente y los derechos constitucionales comprometidos, todo lo cual lo llevaría a la convicción de adoptar una medida que produzca menos perjuicios a los involucrados.

3. Aplicación de la normativa que rige la IFD-RA al caso concreto

La sanción de caducidad de licencia cuyos efectos se suspendieron temporariamente hasta que se agote la vía administrativa, dictada por Resolución N.º 1378/19 del 15 de agosto de 2019, se funda en los siguientes argumentos:

Que el proceder del certificador resulta violatorio de lo establecido en la Ley N.º 25.506 en su artículo 21 inciso *b*, el cual establece la obligación de todo certificador licenciado y de sus autoridades de registro de "Abstenerse de generar, exigir, o por cualquier otro medio tomar conocimiento o acceder bajo ninguna circunstancia, a los datos de creación de firma digital de los titulares de certificados digitales por él emitidos". En otras palabras, prohíbe al certificador licenciado y a sus autoridades de registro acceder bajo ninguna circunstancia a la clave privada de los titulares de certificados.

Asimismo, resulta violatorio de lo establecido en el artículo 19 incisos *2* y *3* relativos a la obligación del certificador de cumplir con lo previsto en sus políticas y procedimientos de certificación y de garantizar la confiabilidad de los sistemas de acuerdo con los estándares aprobados por el ente licenciante, de lo dispuesto en el artículo 21 inciso *3*, el cual repite lo establecido en el artículo 21 b de la Ley N.º 25.506 y lo establecido en el artículo 28 inciso *9* del Anexo al Decreto N.º 182/19 relativo a las autoridades de registro, las cuales deben cumplir con las disposiciones que establezca la Política Única de Certificación y el Manual de Procedimientos del Certificador Licenciado con el que se encuentre vinculada, en la parte que resulte aplicable.

Del análisis de riesgos efectuado sobre los incumplimientos e irregularidades que surgen de los informes mencionados y los elementos

probatorios obrantes en el expediente judicial que tramita ante el fuero penal. La Dirección Nacional de Sistemas de Administración y firma digital de la Secretaría de Modernización, acorde con la conclusión arribada por la SIGEN, recomienda la aplicación de la sanción de caducidad de la licencia en virtud en virtud de haber incurrido el certificador en las causales dispuestas en los incisos *a* y *d* del artículo 44 de la Ley N.º 25.506, específicamente por reincidencia en la comisión de infracciones que dieran lugar a la sanción de multa y por no tomar los recaudos de seguridad en los servicios de certificación.

La sanción ejemplificativa impuesta en caso de hacerse efectiva tendría las siguientes consecuencias:

1) la revocación dentro de los cinco días de notificada la resolución definitiva del certificado digital correspondiente al certificador licenciado Encode S. A.;

2) la imposibilidad del certificador de emitir certificados con efectos de firma digital con posterioridad a la revocación del certificado emitido a su favor;

3) la revocación de todos los certificados emitidos;

4) notificación a los suscriptores y entidades vinculadas;

5) transferencia de la custodia de archivos y documentación e identificación de su custodio;

6) lesiones y perjuicios insuceptibles de apreciación y reparación ulterior para los empleados usuarios y para el propio certificador.

4. Conclusiones

La Infraestructura de Firma Digital en Argentina descansa sobre la confidencialidad de la clave privada del firmante. Dicha clave sólo puede ser generada, almacenada y utilizada por su titular, (generalmente se almacena en un dispositivo criptográfico homologado por la autoridad de aplicación). El certificador no tiene copia de dicha clave, el usuario tiene que tener el control absoluto de sus datos de creación de firma y no puede compartirlos, por lo que debe impedir su divulgación. Ni el certificador ni las autoridades de registro pueden tomar conocimiento o acceder a dichas claves.

En líneas generales, el certificador no puede generar los datos de creación de firma del suscriptor, por lo que al no tener copia de la clave privada del suscriptor. En caso de que dicha clave se pierda, nunca se podrá restaurar, por lo que no queda otra alternativa que proceder a la revocación del certificado correspondiente.

Asimismo, conforme la Resolución N.º 399/16, la cual reglamenta toda la actividad de los certificadores licenciados, se exige que toda la infraestructura tecnológica que soporta los servicios del certificador se encuentre en Argentina y bajo la exclusiva responsabilidad del certificador, por lo que en nuestro sistema no sólo no se permite al certificador crear, tomar conocimiento, acceder a los datos de creación de firma, duplicarlos o bien almacenarlos en sus propios servidores, sino que tampoco se permite almacenarlos en servidores propios o de terceros situados en el exterior.

La firma digital remota en Argentina implica la disponibilización de los certificados y de los datos de creación de firma en un servidor exclusivo administrado por el Estado y situado en nuestro territorio, conforme los estándares tecnológicos y operativos de la IFD-RA, que el mismo Ministerio de Modernización establece como autoridad de aplicación.

La plataforma de firma digital remota, conforme al Decreto N.º 892/2017, es administrada exclusivamente por el Ministerio de Modernización y suministrada en forma gratuita utilizando los procedimientos de firma y verificación establecidos por la autoridad de aplicación de la IFD-RA.

Los certificados de firma digital asociados al uso de firma digital remota son emitidos exclusivamente por la autoridad certificante creada a tal efecto y dependiente del Ministerio de Modernización (AC Modernización PFDR) conforme su política única de certificación.

A diferencia del Régimen de la Comunidad Europea, el cual promueve la firma "en cloud" para crear un mercado digital único europeo basado en el reconocimiento recíproco de todos los certificados de los países integrantes de la CE, con el objetivo claro de agilizar el comercio electrónico y el uso de las aplicaciones móviles,[2] en Argentina sólo el Ministe-

[2] Sólo los prestadores de servicios cualificados en la UE (reconocidos o licenciados, sería en nuestra terminología) podrán prestar servicios de firma "en cloud" y serán distinguidos con

rio de Modernización a través de su autoridad certificación (AC PFDR) puede emitir certificados de firma digital remota conforme su política de certificación. Se trata de un sistema administrado exclusivamente por el Estado que no puede ser implementado por los certificadores licenciados privados dentro de la IFD-RA.

Para mejor comprensión de la situación existente en Argentina y entender cuál es el meollo del presente conflicto, tenemos que tener en cuenta que la Resolución N.º 63/18 de la Secretaría de Modernización, impugnada por inconstitucional por el certificador, establece que a partir de la creación de la plataforma de firma digital remota sólo están homologados para la creación de firma digital de personas los dispositivos de creación de firma por hardware y los dispositivos de creación de firma utilizados por la plataforma de firma digital remota, plataforma administrada exclusivamente por el Estado.

La decisión del certificador sancionado respecto a centralizar en un servidor de su propiedad la emisión de firma digital a favor de sus suscriptores sin lugar a duda supuso una decisión muy arriesgada. Considero que la decisión de cuestionar la Resolución N.º 63/18 antes explicitada y tacharla de inconstitucional es acertada, aunque el ente licenciante varias veces había explicitado su decisión de no autorizar la firma en "cloud" a los certificadores licenciados. Esta decisión discrecional y arbitraria se funda principalmente en la complejidad que implica auditar este tipo de infraestructuras, las cuales integran la infraestructura nacional y podrían incluso ponerla en riesgo.

La decisión tomada por la autoridad de aplicación en línea con la revocación de licencia decretada precedentemente respecto de la empresa Train Solutions no hace más que confirmar la política del Estado de limitar cada vez más la cantidad de certificadores licenciados y reafirmar su decisión de no conceder nuevas licencias a los certificadores que así lo soliciten, lo cual posibilita solamente la constitución de autoridades de registro pertenecientes al sector público o privado, las cuales serán habilitadas previa resolución, siempre que se cumpla con todos los requisitos establecidos por la actual Resolución N.º 42/19.

una etiqueta de confianza.

En síntesis, el mercado de firma digital sigue monopolizado en forma gratuita por el Estado, por lo que no tiene sentido que la iniciativa privada lleve a cabo inversión alguna en tecnología tendiente a constituir una infraestructura de firma digital privada. A lo sumo se recomienda a aquellas organizaciones privadas para las cuales fuera conveniente la utilización de firma digital en sus productos o procesos que se constituyan en autoridades de Registro de la Autoridad Certificante de la ONTI o bien que utilicen el servicio de firma digital remota expedido por la AC del Ministerio de Modernización (AC PFDR).

Lo único prometedor de la actual situación podría ser la introducción de los llamados "servicios de confianza" incorporados por el nuevo Decreto Reglamentario de la Ley de Firma Digital, lo cual podría llegar a generar nuevas oportunidades de negocios, siempre y cuando sus prestadores no tengan que realizar grandes inversiones de dinero para ingresar en este nuevo mercado de prestación de servicios o actividades relacionados con firma digital.

Seminario

PANELISTAS:

HORACIO AZZOLIN
GUSTAVO DALMA
MARINA BENÍTEZ DEMTSCHENKO
DANIELA DUPUY
SANTIAGO GINI
MARÍA JULIA GIORGELLI
PABLO A. PALAZZI
EDUARDO PEDUTO
OSCAR PUCINELLI
SILVANA RIVERO
GUSTAVO TANÚS
JUAN DARÍO VELTANI

Actualización del seminario

Este seminario se realizó en la Universidad de San Andrés el 3 de noviembre de 2017. Todo lo expresado allí guarda actualidad, sobre todo en lo que respecta a los serios vacíos legislativos existentes en materia de violencia de género digital y revenge porn. Ahora bien, entre la realización del seminario y su publicación ocurrieron varios hechos importantes relacionados con la temática abordada.

En 2017 el Congreso de la Nación dio aprobación en el Senado a un proyecto de ley que penalizaba la publicación no autorizada de imágenes íntimas (ver nuestro comentario al mismo en "Consideraciones sobre la aprobación por el Senado de un proyecto de ley para penalizar la publicación de imágenes íntimas", ED *272-563). Sin embargo, durante todo 2018 y 2019 este proyecto no fue tratado en Diputados, con lo cual sigue vigente el vacío en el ámbito nacional.*

Por su parte, la Legislatura de la Ciudad Autónoma de Buenos Aires aprobó una ley sobre difusión de videos íntimos y robo de identidad en diciembre de 2018.

En todo este tiempo, siguen ocurriendo casos de violencia digital online, no limitados al revenge porn sino también vinculado con muchas otras aristas. La ausencia de una ley general específica y la falta a nivel nacional de una sanción penal a la publicación de imágenes íntimas es todavía una deuda del Congreso.

El editor

El derecho a la imagen en Internet y la violencia de género en ambientes digitales

1. Introducción

El 3 de noviembre de 2017 el Centro de Tecnología y Sociedad (CETYS) organizó en la sede centro de la Universidad de San Andrés un seminario para explorar los problemas del derecho a la imagen y la intimidad en Internet y la violencia de género en ambientes digitales. Se convocó a particulares, académicos y funcionarios relacionados con esta problemática, que fue abordada desde el ángulo de las víctimas, desde la violencia de género, y se invitó a funcionarios y académicos a debatir sobre el tema. A continuación se transcribe el programa del evento y la desgrabación de algunos de los paneles.

2. Programa

El derecho a la imagen en Internet y la violencia de género en ambientes digitales. CETYS-UDESA, 3 de noviembre 2017, Universidad de San Andrés, sede UDESA Centro, aula 203.

14.00. Acreditación.

14.30. Presentación. Pablo A. Palazzi, profesor de Derecho UDESA y director del CETYS.

14.45-15.30. Panel 1: Comentario a casos recientes de "Revenge porn".
Marina Benítez Demtschenko, Juan Darío Veltani, Gustavo Tanús.

15.30-16.30. Panel 2: Rol de los jueces y fiscales.
Daniela Dupuy, fiscal Delitos Informáticos CABA. Gustavo Dalma, Fiscalía de Instrucción del Distrito 1 Turno 5 de la ciudad Córdoba. Horacio Azzolin, fiscal Delitos Informáticos PGN.

16.30-17.00. Break.

17.00-17.30. Panel 3: Captación y publicación no autorizada de la imagen. Derecho a la privacidad y protección de datos personales.

María Julia Giorgelli y Eduardo Peduto, Centro de Protección de Datos. Defensoría del Pueblo de la CABA. Oscar Pucinelli, juez Cámara de Apelaciones de Rosario.

17.30-18.00. Panel 4: Rol de los intermediarios de Internet. Problema de la libertad de expresión en Internet.

Silvana Rivero. Santiago Gini, gerente legales OLX-CETYS.

18.00-18.30. Cierre de la jornada.

Pablo A. Palazzi, profesor UDESA, director del CETYS.

3. Paneles

La siguiente es una desgrabación parcial de las ponencias de programa.

Pablo A. Palazzi: Buenas tardes a todos. Me voy a presentar. Mi nombre es Pablo Andrés Palazzi. Soy director del Centro de Tecnología y Sociedad[1] de la Universidad de San Andrés, a cargo de la organización de este evento. Soy profesor de esta universidad en la materia Propiedad Intelectual y Nuevas Tecnologías. También estoy a cargo del Programa de Derecho de Internet y Tecnología de las Comunicaciones que se dicta en esta universidad desde hace ya varios años.

El seminario de hoy es un evento que trata la problemática que está ocurriendo en Internet consistente en el acoso virtual, la difusión no autorizada de imágenes personales e íntimas. Es un fenómeno que se da cada vez más frecuentemente y lo vemos en decisiones judiciales, en proyectos de leyes y en víctimas que a veces lamentablemente no encuentran justicia para su caso. Entonces, la idea fue armar un evento en el cual invitamos a las personas que de alguna forma estén involucradas en este fenómeno, que

[1] CETyS: www.udesa.edu.ar/cetys.

han trabajado como abogados, como legisladores o como funcionarios, e incluso las víctimas, y cuenten un poco lo que están haciendo y de ahí saquemos todos conclusiones de qué es lo que se puede hacer.

El CETYS tiene el Programa académico de Derecho de Internet y Tecnología de las Comunicaciones (DITC), que dura un año y donde tenemos varias materias relativas al Derecho de Internet y las nuevas tecnologías. El año que viene [2018] empieza su cuarto año, al cual están todos invitados.

Ahora les voy a presentar el primer panel de la tarde. En el primer panel se van a comentar varios casos recientes de lo que se conoce como "pornoverganza" o "*revenge porn*", esto es la difusión no autorizada de imágenes íntimas en Internet; en general son imágenes altamente sensibles que son captadas con consentimiento de la afectada pero luego difundidas sin consentimiento de la víctima.

Los oradores de este primer panel son la doctora Marina Benítez Demtschenko y los doctores Juan Darío Veltani y Gustavo Tanús junto con otra de las víctimas en un caso concreto (identificada como M. S.). Así que los voy a dejar con ellos. Cada uno habla diez minutos aproximadamente y después abrimos un poco para debate o para preguntas. Muchas gracias.

Marina Benítez Demtschenko: Mi nombre es Marina Benítez Demtschenko. Muchas gracias por la invitación. Voy a empezar de hoy hacia atrás para ir hilando un poquito cómo es mi historia y como un ejemplo más de todas las mujeres que, atravesando la era digital, somos víctimas de lo que doy en llamar "violencia de género virtual".

Me parece adecuado llamarla así porque el trato que recibimos *online* es el correlato directo del que se nos profiere como mujeres —o del lugar donde se nos coloca— en la sociedad. En general, los agresores son hombres, en un noventa y cinco por ciento; esto no es casual: la imagen de la mujer, la intimidad de una mujer causa morbo, al igual que su sexualidad, en un grado mucho más alto que lo que provoca la desnudez, por ejemplo, de un varón. Ese morbo, presente desde el inicio de los tiempos, perpetúa la acción dañosa, que es acompañada por el resto de la sociedad. Estas características son muy propias de todo tipo de violencia contra la mujer, y no son ajenos al ámbito virtual.

La mujer es la víctima perfecta para destruirla con acciones en Internet que son muy frecuentes y de las que recién se empiezan a cuestionar hace cuatro o cinco años. Antes, esto no estaba visibilizado, y en este orden de cosas es que decidimos, junto con un gran equipo que me acompaña, fundar una organización que se llama Activismo Feminista Digital, de la que soy presidenta.

La fundación lleva adelante el abordaje, la investigación, el tratamiento de casos de violencia de género virtual entre los cuales principalmente tenemos dos causas de consulta, siendo casi el noventa por ciento de los casos que recibimos para asesorar. Por un lado, la difusión no consentida de material digital íntimo y, por otro lado, el acoso virtual "propiamente dicho" —como lo denominamos—, que tiene que ver con el acecho, la persecución, el hostigamiento de una persona hacia otra a través de los medios digitales o plataformas virtuales (que comprende los servicios de mensajería instantánea, el *e-mail*, teléfono, celular y demás).

¿Cómo llego a ser presidenta de esta fundación? Mi experiencia en el trabajo de campo data de ya casi seis años, porque en realidad yo fui víctima de la difusión no consentida de mi material íntimo por parte de mi ex pareja en 2011. Al finalizar un noviazgo de casi cinco años, padecí un período de mucha violencia psicológica. Nunca me animé a denunciar porque también tenía mucha vergüenza. Yo estaba en ese momento iniciando mi carrera como abogada, a dos años y medio de recibida, pero que recién comenzaba a darme mis frutos económicos propios y capital social, ejerciendo de forma independiente como lo hago ahora. Después de esos cinco o seis meses de violencia psicológica directa, me empezaron a cruzar hombres por la calle haciendo referencia a que me conocían, que les daba gusto verme "finalmente". Sabían todo de mí, principalmente datos personales muy privados, familiares, de mucha intimidad. Con el tiempo los encuentros "casuales" comenzaban a ser más invasivos. Me abordaban, me tocaban, me tiraban del pelo, me querían besar o directamente me besaban sin que yo los habilitara. A los tumbos, a la fuerza; todos eran sorpresivos, arrebatados, y mi terror aumentaba cada vez que salía a la calle.

He padecido situaciones muy difíciles de sobrellevar, máxime sabiendo que yo no sabía de dónde venía todo esto. Un año y medio transcurría desde iniciada esta oleada de acosos y abusos por parte de cientos

de hombres en la ciudad de La Plata, un año y medio en el que viví un infierno, en el que dejé mi profesión, en el que me encerré en mi casa porque tenía miedo de salir, en el que además sufría trastornos alimenticios y de sueño, etcétera.

Cuando restringí mis salidas a la calle porque ya era insostenible el nivel de acoso que recibía de parte de hombres que sabían todo de mí, empecé a recibir acosos por teléfono y en mi cuenta personal de Facebook, que tenía mi nombre. Me llegaban mensajes, solicitudes de amistad, me abordaban de todas las formas posibles. Llamadas a cualquier hora de la noche. Cambié seis veces el [número de] teléfono; las seis veces fueron obviamente con esta causa de trasfondo, porque me llamaban números que yo no conocía y era constante la situación de acecho.

Hasta cierto momento nunca lo hilé con mi ex pareja y con esta ruptura tan cargada de violencia que contaba anteriormente. Al año y medio de todo este padecimiento, me obligué a volver a salir a caminar por la calle. Ya estaba haciendo tratamiento psicoterapéutico y necesitaba de alguna forma retomar mi vida, que se había truncado por hechos que no podía entender por qué se generaban contra mí. Después de, repito, un año y medio. Esto había empezado en junio de 2012 y la primera vez que volví a caminar sola fue en diciembre de 2013.

Cuando decidí intentar salir de mi encierro, ese mismo día también fui abordada por otro hombre que esta vez enfrenté. Lo insté a que me respondiera de dónde me conocía, porque todos los hombres tenían la misma metódica de abordaje y me daba cuenta de que él era parte de lo que todos los demás también hacían. La metódica era la siguiente: me llamaban por mi sobrenombre —que era "Kiki", el sobrenombre que mi ex pareja, Sebastián Horacio Masi, me había puesto en su momento durante la relación—. Luego, todos me instaban a tener un encuentro sexual. Yo al principio pensé que me los mandaba él para perseguirme, pero este último que me animé a enfrentar me dijo que no: que había un perfil en la red social Facebook que se hacía pasar por mí. Puntualmente me dijo: "Hace diez meses que nosotros chateamos", haciendo referencia a que era yo la persona con la que él intercambiaba mensajes eróticos y fotografías sexuales. Yo me quedé helada, le dije que en realidad no era yo y acto seguido le pedí colaboración para hacer la denuncia; salió corriendo, me dijo que era casado, que no quería

saber nada, que era una loca. Así fue cómo tomé conocimiento con certeza de que había un perfil, una cuenta creada que se hacía pasar por mí pero que no llevaba mi nombre, por eso no la podía ubicar.

En abril de 2014 me llama un vecino de la casa de mis padres, que viven a diez kilómetros de la ciudad de La Plata. No era una persona con quien yo tuviera contacto, de hecho no lo veía desde mi infancia. Me alerta que había un perfil en Facebook que decía ser yo y que estaba ofreciendo fotos íntimas mías. Lo había contactado. Esas fotos existían y eran producto de nuestra intimidad como pareja de cinco años de relación, pero obviamente no existían para la difusión. Existían para que sea compartidas entre quienes estaban destinadas a serlo. Por eso todo este proceso tuvo un extra de esfuerzo psíquico para mí: entender que no debía sentirme culpable por ello.

A ese vecino que se comunica conmigo le pido por favor que le siga el juego a esta cuenta que lo había contactado como a tantos hombres. Se lo sigue, se muestra interesado en la propuesta y logra que del otro lado le dieran un teléfono, al que llama. El resultado es una comunicación de cuarenta minutos con mi ex pareja, Sebastián Masi, la cual graba, en donde este último le confiesa que en realidad se estaba haciendo pasar por mí porque yo también estaba detrás de este juego y él se encargaba de contactar hombres para que yo pueda concretar diversas fantasías sexuales mías. Entre ellas, encuentros sexuales múltiples.

En ese momento hilé que durante casi dos años ya, el pretenso "juego" era mandarme hombres todo el tiempo, bajo el perfil de Facebook que se llamaba "María de los Ángeles Rivera", incentivando a estos hombres a que me conocieran entera, no sólo físicamente. Sabían dónde vivía, qué hacía, dónde trabajaba, a qué hora salía del trabajo, quiénes eran los miembros de mi familia, los teléfonos celulares, los teléfonos de mi familia. Para asegurarse de que su identidad no fuese revelada, se hacía pasar por mí y hablaba como yo, convenciendo a todos de un pleno consentimiento mío en toda esta artimaña, un consentimiento que obviamente jamás había prestado. Mucho menos teniendo en cuenta que, para esta altura, ya hacía más de dos años que había terminado el vínculo y me había alejado de él sin volver a verlo jamás. La cuestión es que con este testimonio —o sea, con la grabación de cuarenta y cinco minutos— logré radicar la cuarta denuncia

en la Comisaría de la Mujer de La Plata; las tres primeras habían resultado frustradas, ya que me dijeron que como lo que estaba padeciendo no era un delito (yo para esa altura ya lo sabía, era abogada hacía casi tres años para ese momento), con ese panorama lo único que podía hacer era radicar una exposición civil, que por supuesto no tiene efectos jurídicos.

Cuando voy con la grabación, me toman finalmente la denuncia y "me sugieren" la petición de una medida cautelar de prohibición de acercamiento. En mi asombro, le respondo: "¿Contra quién?", porque no tenía certeza tampoco de que mi ex pareja fuese el único implicado, o si había más personas; no sabía si los que venían a abordarme estaban implicados también.

Esto es una muestra muy cabal del desconocimiento de los operadores policiales en el campo de los delitos informáticos. Obviamente las Comisarías de la Mujer deberían estar capacitadas para receptar esta problemática de forma útil y hábil, sabiendo que este tipo de violencia es tan frecuente, pero tampoco lo están. Pasaron casi seis años de ese momento y seguimos más o menos igual.

Al día de hoy también se encuentran renuentes a incorporar no solo estos conocimientos sino también las modalidades en que se lleva adelante la violencia digital hacia las mujeres.

Me presenté con un abogado penalista en la ciudad de La Plata en julio de 2014. Me constituí como particular damnificada: quise intervenir activamente en la propulsa de las actuaciones y así lo manifesté todo el tiempo, ya que desde el momento en que me había encerrado en mi casa, me propuse presentar un proyecto de ley. Y había estudiado lo suficiente como para plantear estrategias y hacerle frente a esta problemática desde un lugar absolutamente innovador, como no se había hecho en Argentina hasta ese momento. Yo sabía que iba a lograr un camino para otras mujeres que estuvieran padeciendo este flagelo, y que era necesario hacerle frente y batallar en múltiples flancos, principalmente para visibilizar el carácter absolutamente destructivo de la violencia digital.

La violencia digital te coloca en un lugar no solo de máxima vulnerabilidad, sino también de mucho temor, de mucha inseguridad. Yo lo que temía era que me violen, que alguno de estos hombres se enganche con esta historia y que vaya más allá. En mi peor momento psicológico me

incentivé a estudiar y a redactar un proyecto de ley para penalizar estas conductas. Y lo hice. Lo presenté este año [2017], o sea, cuatro años después de todo lo ocurrido, porque recién en 2016 se empezó a hablar en los medios de comunicación de la violencia de género virtual y, puntualmente, de la difusión no consentida de material íntimo. Antes de 2016 los legisladores y las legisladoras no hicieron caso a mis planteos insistentes. No les parecía grave; ni siquiera les parecía que fuese un tema de agenda, una indiferencia similar a la que se le ha proferido al abordaje de los ciberdelitos en general, que en el mundo son objeto de tanto estudio y abordaje académico, doctrinario, jurisprudencial. En Argentina estamos recién tomando cierto conocimiento de esta cuestión hace dos años.

El proyecto de ley que presenté, prevé la tipificación de varias aristas de la violencia de género digital:

1. La difusión no consentida de material íntimo, aún cuando hubiese sido obtenido con el consentimiento de la víctima, que es como en realidad se da: se da en un marco de confianza y, por ende, con una expectativa de confidencialidad entre las partes intervinientes —parejas o no parejas, situaciones íntimas espontáneas—. Es muy importante hablar de esto: la expectativa de confidencialidad y privacidad al prestar nuestra imagen en ese juego, y respecto de quiénes lo prestamos, en qué condición, en qué modalidad. El tipo penal está planteado para perseguir y condenar a quien difunda ese material sin el consentimiento de la víctima. *La obtención es con el consentimiento, la difusión es sin el consentimiento*.

2. Planteo además la tipificación del acoso virtual, esto es el acecho, la persecución, no necesariamente un hostigamiento simple. Acá, en la Ciudad Autónoma de Buenos Aires, la conducta está prevista como una contravención, pero en la provincia de Buenos Aires y en el resto del país no tenemos esa herramienta. De hecho, no existe ni la figura del acoso ni la figura del hostigamiento, así que no tenemos nada. Si realmente hay actos constantes de persecución con claros fines de molestar, de lograr algún objetivo abstracto (no importa cuál), la persecución per se es lesiva del derecho constitucional del libre tránsito. Para las mujeres también esto es muy difícil, por eso también se ha llevado adelante la lucha feminista de lo que se denomina el "acoso callejero". En sumatoria, esta figura llevada al Congreso para su tratamiento parlamentario exhibe

una realidad: el acoso virtual como acecho y persecución —por medios digitales— en general termina obligando a la víctima a alterar su proyecto de vida o su cotidianidad, lo cual supone una gravedad suficiente para pedir la tutela del Estado, es decir, que sea condenada también con prisión. Tanto el acoso virtual propiamente dicho como la difusión no consentida de imágenes íntimas deben ser condenados con prisión: la previsión que tuvimos para definir esto es que se les dé la jerarquía de delitos de orden público.

¿Qué pasa en la justicia con cuestiones relacionadas con violencia de género? Yo soy feminista, hace más de quince años: antes de dedicarme a lo que son los ciberdelitos, llevé adelante muchísimas causas relacionadas con violencia doméstica, violencia de género, en otros ámbitos en la vida cotidiana. Y toda esta cuestión, si bien además es muy subestimada en la justicia (una justicia absolutamente machista, también es perseguida mediando una figura débil del fiscal o de la fiscal. Una figura que exige ser acompañada consecuentemente por la víctima constituida como particular damnificada, o sea, una víctima que en el medio de su ruta crítica, es imposible que tenga la lucidez para proponer prueba, para hacer un *racconto* preciso y detallado de los hechos dañosos, para relacionar ideas, para proponer medidas, para brindar información ordenada. Y eso también lleva a que la generalidad de los casos de violencia de género doméstica que se judicializan sean tomados como delitos "livianos". La instancia privada en que se encausan los delitos que afectan la privacidad y la intimidad supone obligar a una víctima a que salga de su estado de vulnerabilidad y que se ponga firme para perseguir la investigación. Y esto es una doble victimización, una situación que repudio, algo que he visto siempre; incluso la veo cuando los mismos fiscales proponen que la víctima venga a hablar con ellos todo el tiempo.

En el proyecto de ley preveo que estas conductas dañosas antes reseñadas sean delitos de orden público. Esto supone que la tipificación de la difusión no consentida de material íntimo y del acoso virtual insten una investigación penal en que los fiscales se constituyan como figuras fuertes en la propulsa, y sean quienes piensen por la víctima, quienes cumplan un rol tuitivo; que sean los que hilen las pruebas, los relatos; que animosamente propongan prueba, estudien, se capaciten como en otros lugares

del mundo. Acá eso no pasa. Esto es una forma también de articular medidas protectorias efectivas desde el Estado, en consonancia con la Ley 26.485 contra la violencia hacia las mujeres. Esta ley es fundamental no solo para cualquier íter o cualquier camino procesal que se proponga, sino también para el planteo de políticas públicas: todo avance del Estado —a nivel social en materia de protección de los grupos puestos en situación de vulnerabilidad— tiene que tener sí o sí una correlación directa con esta ley, que además es el producto de una lucha mundial de las mujeres por el reconocimiento de sus derechos, que es en definitiva la bajada operativa de la aplicación de los pactos internacionales que prevén una tutela específica para las mujeres.

La perspectiva de género, lineamiento del que escuchamos todo el tiempo comentarios como: "perspectiva de género… feminismo… ¡cómo está el feminismo!", supone un análisis vital del caso; supone el tratamiento diferenciado según la víctima: su carácter, su condición social y cultural en cuanto al posicionamiento de género. No son lo mismo las consecuencias sobre un hombre víctima —que también sufre de por ejemplo una difusión no consentida de su material íntimo y de acoso virtual— que las que padece una mujer. Incluso la perspectiva de género supone contemplar con otro prisma los casos en que no son víctimas mujeres sino que son personas del colectivo LGTBIQ[1]. Ellxs están colocadxs en un lugar de máxima vulnerabilidad agravado por el hecho de que además no se ha logrado aún la visibilización de la problemática que les ocupa en este ámbito de lo digital.

Las mujeres hemos librado una lucha muy sólida, patente, fuerte: no nos callamos más, pero los colectivos vulnerables todavía están en esa área gris por no animarse a hablar o simplemente por saber que se les profiere un tratamiento absolutamente descalificador. A esta situación la vemos reflejada asimismo en los casos que nos llegan a la fundación. El tratamiento que se les profiere ante una denuncia, por ejemplo, da cuenta de una aminoración en la respuesta estatal.

¡Hay tantos conceptos que tenemos que poner sobre la mesa, de los que tenemos que empezar a hablar realmente! Dónde estamos parados y paradas; quién puede juzgar cuál es la expectativa de privacidad que

[1] LGTBIQ: Lesbianas, gays, trans, bisexuales, intersexuales y queer.

cada persona tiene, etcétera. Claramente hay una premisa subyacente: desde el momento en que yo comparto con quien comparto un momento íntimo, es esperable que fuese solamente entre los participantes. Eso me parece lógica lisa y llana. Pero para el machismo, que se actualiza y perfecciona cíclicamente para perpetuar la opresión ejercida, no lo es. De hecho, la intimidad de las mujeres en la era digital es un medio muy efectivo de destrucción.

Yo la pasé muy mal, no solo por el lado de lo que estaba viviendo y del temor (de ver afectada mi integridad sexual, física, mi integridad psíquica, ya en ese entonces absolutamente alterada) sino también por el descreimiento del Sistema. Yo siempre digo lo mismo: una víctima que tiene que enfrentarse todo el tiempo a decir su verdad para lograr algún mínimo de protección, es de una crueldad atroz.

Al día de hoy, yo sigo litigando contra mi agresor… seis años después: eso es "el Sistema". Eso es el descreimiento del Sistema hacia la víctima. Y digo una frase de cabecera que es horrible pero es la realidad puesta en palabras para visibilizar qué es lo que pasamos quienes elegimos judicializar problemáticas de violencia de género: "Yo tengo dos enemigos, dos entes contra quienes tengo que batallar todo el tiempo: mi agresor y el sistema judicial". Y además el Poder Ejecutivo, que desoye la exigencia de políticas efectivas y fuertes contra la violencia hacia las mujeres; y el Poder Legislativo, que es renuente a incorporar conceptos como estos, de abrir el recinto para darles tratamiento a problemáticas complejas, e incluso renuente a siquiera tratar de entender los lineamientos de acción a favor de los grupos puestos en situación alarmante de vulnerabilidad, que podemos acercar los organismos no gubernamentales —lxs que estamos en el campo, que tenemos contacto directo con el sistema, las víctimas, las carencias, las necesidades—.

Pero es una tarea ardua, difícil: a veces incluso me la planteo como imposible. Yo me tengo que enfrentar, por ejemplo, a plantear una medida de protección en el expediente —porque mi ex pareja al día de hoy sigue desobedeciendo la perimetral que le insté hace cuatro años—, y el sistema me dice "bueno"; el Poder Judicial me dice "Bueno, pero mientras él no te haga nada, no hay problema en que se acerque". Y yo le digo: "¡No! ¡Son doscientos metros de prohibición de acercamiento, donde no puede estar

parado en la zona en donde yo estoy!". Todo el tiempo así. Eso es el Sistema. Se suman para agravar el panorama de las víctimas, las dilaciones temporales; los proveídos que tardan en salir —por los menos en provincia de Buenos Aires—, veintinueve días. En veintinueve días nos pegaron cinco tiros a las víctimas de violencia doméstica, casos acuciantes como el mío.

Es muy común no entender nada de todo esto; la falta de información es también parte de un Estado indolente. Por ejemplo, la diferencia entre "violencia doméstica" y "violencia de género", que son conceptos unidos en una relación de especie-género. Hablar abiertamente del estado de vulnerabilidad de las mujeres, que socialmente tenemos un lugar de opresión y que por ello resultamos más frecuentemente víctimas, y más pasibles de ser destrozadas. Un lugar en donde la sociedad entera colabora a la violencia hacia nosotras.

La difusión no consentida de material íntimo en formato digital no es la excepción de esto que estamos hablando; cuando vemos en los grupos de WhatsApp de varones que de repente se mandan videos amateurs de chicas y hombres teniendo relaciones sexuales, pero que se visualiza en general únicamente a la mujer: ¿algún varón se ha cuestionado si tal video pudo haber sido puesto a disposición sin consentimiento de la persona implicada?

Cómo evitamos la viralización —la difusión irrestricta, ilimitada a indeterminada cantidad de personas— hace no sólo al uso responsable de las plataformas virtuales o redes sociales, sino también a la concientización sobre los ciberdelitos contra derechos personalísimos: la intimidad, la privacidad, la integridad psíquica, física, sexual, la dignidad, la libertad en sus múltiples aristas. Es una oleada activista que tenemos que receptar como país. Un país bastante atrasado.

En su momento, cuando fui a hablar con, en aquel entonces, la persona a cargo de la División de Delitos Tecnológicos de la Policía Federal, estando muy bien ubicado y haciendo ya tareas de prevención y abordaje primario en ciertas cuestiones relacionadas con ciberdelitos, ante mi planteo desesperado sobre qué podía hacer frente a lo que me estaba pasando, me dijo: "Y no… qué querés que te diga; yo te diría que te la banques y en algún momento se le va a pasar". Esa es la respuesta constante a las víctimas de violencia de género y doméstica: al agresor "ya se

le va a pasar". Hay que entender también la psicología de los agresores y las víctimas, y las connotaciones sociológicas detrás de la violencia de género y doméstica. Esto es una problemática que implica que las mujeres estamos constituidas como objeto de explotación de los agresores: hasta no lograr la explotación total, y eventualmente la destrucción, *no paran.*

Parece que el Sistema no se ha enterado de este concepto todavía porque también propone lo mismo: dejarlo pasar, archivar las causas, proveídos de veintinueve días, llamar a la víctima nueve o diez veces para que declare lo mismo —porque no les anda la computadora o porque no entendieron muy bien una parte—. La doble victimización está reflejada en todo el recorrido adicional —y casi siempre, innecesario— que tenemos que hacer pasar a una víctima para escuchar su verdad y reaccionar en contra de su agresor.

La fundación actualmente tiene una conformación de mujeres y de varones. Los varones están instruidísimos en perspectiva de género: es una exigencia el conocimiento de nuestros integrantes sobre cómo opera la desigualdad social entre hombres y mujeres; las consecuencias que una víctima mujer tiene en un caso determinado de violencia digital y las que padecería la víctima siendo hombre; la estimación justa sobre las connotaciones que se presentan en uno y otro caso, y que no podrían recibir el mismo tratamiento sin reproducir una gran injusticia, es vital. Las mujeres necesitamos una tutela extra; el hombre acosado no ve en peligro su integridad sexual, por ejemplo; la mujer acosada, sí. Y esto no quita que es muy cierto que hay varones que padecen estas problemáticas, pero hay que estar plenamente conscientes de que en estos casos su padecimiento gira sobre la lesión a su honor, y lo que implica en el nuestro es el peligro sobre nuestra vida.

Definitivamente es un camino que recién empieza. Es un camino muy arduo, que implica que lo tengamos que explicar a cada paso que vamos. Gracias a que tenemos también una lucha feminista muy fuerte, podemos incorporar esto y podemos lograr de a poquito la apertura de todos y de todas para poder receptar cada arista de estas problemáticas… cuestionarnos cada día algo más, principalmente problematizando las construcciones socioculturales impuestas, que son tan sólidas que parecen irrompibles.

La violencia digital no es simplemente un "mostraron mis fotos" o un "me llama diez veces por día", sino que es la antesala de violencias

mayores, que en general derivan en violencia física o violencia sexual. Tengamos como ejemplo diez casos que puedo llegar a pensar ahora que han llegado a la fundación: cuatro conllevan también situaciones de violencia física; la mitad tiene una raíz de violencia doméstica (dada entre parejas o agresores que son ex parejas).

Los casos que llegan a consulta en la fundación nos permiten intermediar con conocimientos en el campo, pero como somos una organización no gubernamental, nuestras herramientas son limitadas, y por más que brindemos información, contención y asesoramiento en momentos vitales, nos frena nuevamente el accionar indiferente del Estado. Y ahí es donde el agresor ataca, y ataca certero. Y ahí es donde están todos los casos que vemos constantemente en la televisión… de los que nos horrorizamos, nos indignamos y respecto de los que salimos a hacer campaña luego.

La pregunta es: ¿cuándo vamos a empezar a tratar esto con el conocimiento y con el abordaje que realmente requiere? Es importante estar preparadxs desde el momento en que la víctima viene a hablar con nosotrxs. Estas problemáticas insumen muchísimo tiempo, entonces es importante dedicarle a cada situación su espacio y respeto; afinar el oído, dando más lugar al testimonio de la víctima y estudiando el campo de la violencia hacia las mujeres. Animémonos también a hablar de que la violencia digital hacia las mujeres, principalmente la difusión no consentida de material íntimo, es violencia sexual, también violencia psicológica.

Mi causa actualmente está planteada como "lesiones psicológicas graves en el contexto de violencia de género". Tampoco parece convencer a la justicia. Yo estuve cinco años y medio con tratamiento psicológico, pero aún así no parece ser una motivación para que la justicia actúe; mi agresor al día de hoy sigue dando vueltas, sigue trabajando en el mismo lugar. Trabaja en el Ministerio de Seguridad de la Provincia de Buenos Aires, es empleado administrativo, pero trabajó en armamento durante veintiocho años. Tiene contactos muy peligrosos y además tiene causas por portación de armas ilegítimas. Una de ellas fue cuando le allanaron el domicilio en ocasión de mi denuncia, que es el expediente que estoy llevando adelante al día de la fecha.

Es un camino difícil, pero con el mero hecho de que podamos ser conscientes de que no estamos frente a casos de "loquitas que se sacaron

fotos y el noviecito se las viralizó", ya es un gran paso. Estamos siempre enfrente de mujeres que son puestas a disposición de terceros en su intimidad y en su sexualidad, y eso tiene una capacidad dañosa inconmensurable, porque además lo que hace es lograr el objetivo esperado por el agresor: aislarla, lograr su descreimiento y lograr una reacción social en contra de ella para que directamente no pueda volver a reconectarse socialmente. Es un medio de violencia psicológica absolutamente efectivo.

Así que solamente [quiero] plantearles esta idea, instarlos al autocuestionamiento: instalemos la exigencia, de acá en adelante, de llamar a las cosas por su nombre. Y hablar de esto como lo que es: es violencia de género virtual. Es una nueva modalidad de un problemática histórica, que es la violencia hacia las mujeres.

Eso es todo lo que tengo para decir. Muchas gracias.

Gustavo Tanús: Buenas tardes. Yo les voy a contar un caso relacionado con estos temas y en el cual me tocó actuar como abogado de la víctima. El caso se resolvió a fines del año pasado. Por lo que cuenta Marina [Benítez Demtschenko] y lo que estuve hablando con los restantes panelistas del día, este caso es distinto porque no se llegó a concretar la "porno venganza", sino que se pudo evitar.

Es un caso de una chica, una fiscal recién nombrada en Brasil, que hacía dos años que estaba de novia con un chico que trabaja acá en el Poder Judicial. Bastante jóvenes, relación a distancia. *Mail* va, *mail* viene, WhatsApp, mensaje con fotos, videos íntimos para mantener viva la relación.

Llegó un momento en que tras dos años de la relación, esta se termina, por decisión de la mujer, y a partir de ese momento ella empezó a recibir mensajes de *mail* y de WhatsApp amenazándola, diciéndole que si no volvía con él, todo el Poder Judicial de Brasil se iba a enterar de sus fotos y sus videos. Ella pensó que era una cuestión de bronca y que se le iba a pasar, pero cada vez el acoso era mayor y la violencia era mayor. Cuando ella le decía que iba a hacer algo, él se ponía peor, y aparte decía que él trabajaba acá en el Poder Judicial, que nadie iba a poder hacer nada.

Frente a esto la víctima toma la decisión de iniciar acciones legales. Primero había sido denunciarlo penalmente. Justo la expositora anterior hablaba de hostigamiento acá en la Ciudad de Buenos Aires. Pero la

víctima estaba en Brasil, demostrar el daño acá en la Argentina, fin de año, y presentar la denuncia contravencional, ratificarla y lo que sea, va a pasar el tiempo y tal vez se termina concretando lo que no queríamos que se concretara.

Entonces se nos ocurrió recurrir a la figura del Código Civil y Comercial, el nuevo, el artículo 1.711, que contiene la acción preventiva de daños,[2] que establece que cuando hay una probabilidad cierta de que un daño se produzca o se siga produciendo, se puede iniciar una acción preventiva para tratar de evitarlo o por lo menos que el daño que se haya producido cese.

La decisión fue iniciarlo y por esa vía, no por el lado penal, para ver si se obtenía algún resultado. Pero ahí no terminó la cosa. El primer problema fue decir en qué fuero lo iniciamos, porque esta era una cuestión de Internet, y en muchos casos este tipo de reclamos resulta competencia de la justicia civil pero a veces de la justicia federal. Lo iniciamos en el fuero civil y comercial federal, y lamentablemente el juez interviniente, no solo por la cuestión de Internet sino también porque era un conflicto entre un ciudadano de otro país y un ciudadano argentino, se declaró incompetente. Pensamos que cuestión federal era más clara que por vía civil, pero el juez se declaró incompetente y remitió el caso a la justicia civil. Ya se acercaba fin de año, el temor era que las fotos finalmente se publicaran. Decidimos no apelar la medida, el expediente pasó entonces a un juzgado civil y en diciembre del año pasado el juzgado civil a cargo del caso hizo lugar a la medida como acción preventiva, cautelar, una mezcla medio rara, pero que ordenó que el chico que tenía las fotos íntimas se abstuviera de reproducirlas, se abstuviera de difundirlas, y dejara de acosarla a ella enviándole mensajes y amenazándola.

Acto seguido iniciamos una mediación contra el autor, reclamándole los daños y perjuicios y, aparte, que esa cautelar quedara firme, que fuera definitiva. Pero, bueno, no hizo falta porque él se presentó espontáneamente… espontáneamente no, fue notificado de la medida y se presentó, se allanó. Incluso llegamos a un acuerdo indemnizatorio en el que a su

[2] Artículo 1.711. Acción preventiva. La acción preventiva procede cuando una acción u omisión antijurídica hace previsible la producción de un daño, su continuación o agravamiento. No es exigible la concurrencia de ningún factor de atribución.

vez se comprometió a eliminar todas las imágenes y los videos de su sistema, y no se concretó pero quedó a disposición para que se hiciera una medida para comprobar que en ningún dispositivo electrónico él tenía ya fotos y videos de ella.

Como ven, no es un caso de "porno venganza" consumado, pero entiendo que la acción preventiva del nuevo Código Civil puede llegar a ser una vía útil y efectiva para cuando una persona tiene sospechas de que alguien tiene imágenes íntimas de uno, y puede llegar a utilizarlas, demostrándolo de alguna manera. Nosotros teníamos bastantes cosas para demostrarlo, pero también siempre es difícil si el *mail* realmente lo mandó él o no, si el mensaje de WhatsApp estaba grabado, lo tiene en el celular, etcétera.

No hizo falta esperar a que el delito se consumara y que el daño ya se produjera, más allá de que ella sí tuvo un daño como quizá Marina, todo el tiempo que pasó con el miedo a que se difundieran las imágenes. Pero se pudo evitar de esta manera.

Cuando me convocaron a hablar estos temas, preferí comentarles este caso. Como las partes son confidenciales, por eso tampoco nunca fue publicado, pero es de un juzgado civil de fin del año pasado [2016], y que demuestra que a través de esta acción preventiva se puede llegar a evitar que se produzca un hecho de estas características.

Hay que tener en cuenta que el nuevo Código Civil y Comercial contiene un artículo 52 y otro artículo 53. El artículo 53 reconoce el derecho a la imagen en forma autónoma al derecho a la privacidad.[3] El artículo 53 se refiere al derecho a la dignidad.[4] De estas normas surge que para captar o reproducir una imagen hace falta el consentimiento de la persona. En este caso el consentimiento no estaba dado para ser

[3] Artículo 53. Derecho a la imagen. Para captar o reproducir la imagen o la voz de una persona, de cualquier modo que se haga, es necesario su consentimiento, excepto en los siguientes casos: a) que la persona participe en actos públicos; b) que exista un interés científico, cultural o educacional prioritario, y se tomen las precauciones suficientes para evitar un daño innecesario; c) que se trate del ejercicio regular del derecho de informar sobre acontecimientos de interés general. En caso de personas fallecidas, pueden prestar el consentimiento sus herederos o el designado por el causante en una disposición de última voluntad. Si hay desacuerdo entre herederos de un mismo grado, resuelve el juez. Pasados veinte años desde la muerte, la reproducción no ofensiva es libre.

[4] Artículo 52. Afectaciones a la dignidad. La persona humana lesionada en su intimidad personal o familiar, honra o reputación, imagen o identidad, o que de cualquier modo resulte menoscabada en su dignidad personal, puede reclamar la prevención y reparación de los daños sufridos, conforme a lo dispuesto en el Libro Tercero, Título V, Capítulo 1.

difundido, sino que estaba dado en el marco de la relación privada entre las partes. Una vez terminada la relación, si se quiere usar la imagen para otra finalidad, debería haber tenido el consentimiento de ella. Claramente no lo tuvo, y ahí estaba la potencialidad del daño que permitió que se configure la posibilidad de iniciar la acción preventiva.

Bueno, nada más que comentarles eso. Gracias a todos.

Juan Darío Veltani: Buenas tardes. Mi nombre es Juan Darío Veltani, soy un abogado que se dedica a temas de tecnología hace mucho tiempo, en todas las áreas, disciplinas del Derecho que toquen en un punto a la tecnología, y cada vez son más.

En ese contexto, lo conozco hace quince años por lo menos a Pablo Palazzi, estamos trabajando siempre en temas académicos en conjunto. Con Gustavo Tanús, también. Y cuando se organizó este seminario, Pablo, que sabía que yo había llevado adelante un tema vinculado con *revenge porn*, me invitó y Pablo [Palazzi] me dijo —yo lo veo con buen criterio— que sería interesante que también escucháramos a la víctima, no solamente que la escuchen los jueces y demás, sino que la veamos y la escuchemos. De modo tal que a mi izquierda está M., que es la víctima de mi caso, o del caso que llevamos nosotros en el estudio. Entonces, previo a todo, aclararles que no es que tenemos una casuística tremenda y llevo trescientos casos de *revenge porn*. No, porque no es a lo que nos dedicamos. Llevamos el caso de M. Fue un tema especial, y la verdad es que, como ahora les voy a comentar, salvo unas cuestiones que tienen que ver con el sistema pero más globalmente, nuestra visión es bastante positiva respecto a lo que nos encontramos en la justicia. Nosotros. Pero es un caso.

Pero les quiero adelantar que este caso ha dado una multiplicidad de ramificaciones porque el daño que se genera con el *revenge porn* o la violencia de género en Internet no se agota a veces con solamente encontrar a quién publicó o quién subió inicialmente el video: los efectos de la viralización son dañosos y siguen ocurriendo y es tremendo, es desesperante para quien lo sufre, y para quien tiene que asistir a quien lo sufre, porque en definitiva uno intenta darles respuestas con las herramientas procesales que tenemos. Es desesperante cuando uno advierte que las cosas están pasando en Internet y no podemos hacer nada al respecto, o es muy difícil detener lo que pasa en internet.

Entonces, la aclaración que les quiero hacer es que la causa a la que me voy a referir es una causa penal, una causa que está prácticamente terminada —digo "prácticamente" porque cuando les cuente en qué está, ahí está mi crítica al sistema penal en general—, no me voy a referir a todos los aspectos civiles, que son otros aspectos que merecen otra mesa y otra discusión. Solamente lo penal.

En ese contexto, primero les cuento básicamente los hechos. Después le voy a dar la palabra a M. para que ella nos dé su visión, que ella lo sufrió en carne propia. Lo mío fue conocerla y conocer estos hechos.

Ella estaba en una relación de pareja. A fines de noviembre de 2012 decide terminar esa relación de pareja. Cuando termina esa relación, su pareja la empieza a extorsionar, de distintas maneras, pidiéndole, básicamente, que ella le diera un dinero, porque ellos habían planificado un viaje en común que después se frustró, con motivo de la decisión de ella de terminar su pareja, y que si no le daba ese dinero, él iba a publicar un video íntimo que ellos habían filmado en el ámbito de la pareja.

Tanto la hostiga, la persigue, la llama a ella, a los familiares, amenazas, la verdad es que es bastante compleja esta primera parte de los hechos, pero lo relevante es que ella accede al pedido y le paga este dinero para que el señor no publique ese video, y terminar de un modo con esto.

Bueno, lo que ocurrió es que la persona esta publicó el video igual. A pesar de haber recibido el dinero, lo publicó. Publicó no solamente ese video, sino otro video más, que había en una computadora que ella tenía y que ella consideraba haber borrado. Él era técnico informático, con lo cual él sabía perfectamente lo que hacía. Él había obtenido el video sin que ella lo supiera, publicó los dos videos. Los editó, los publicó, cosificándola a M., es decir, transformando lo que era una acto íntimo en un acto no íntimo, poniéndola a ella en una situación bastante desagradable. Y se encargó de que en el lugar donde vive M., que es un pueblo de treinta mil habitantes, a seiscientos kilómetros, en la provincia de Buenos Aires, se encargó de que en ese pueblo de treinta mil habitantes todo el pueblo supiera, el diario local, todo el mundo supiera que había un video, dónde estaba el video y que el video era el video de M.

M. es contadora, tiene una hija pequeña y en el momento de los hechos daba clases en el colegio secundario del pueblo. Cuando nosotros

accedemos a tomar la causa —porque, insisto, no es que nos dediquemos a este tipo de causas pero sí hacemos tecnología en general, decimos, bueno, hay varias cuestiones que plantearse frente a esto.

La primera cuestión es la competencia. ¿Cuál es la competencia para entender en esta causa, la persona, la deberíamos imputar? Porque nosotros sabíamos perfectamente quién había subido el video sin perjuicio de que luego hubiera que probarlo. Y que él lo había subido originalmente, porque luego se demostró que hubo otros que lo resubieron y después se viralizó, y después, por efecto de los buscadores, se terminó, digamos, difundiendo por todos lados.

Pero el original… lo sabíamos. Entonces, ¿la competencia dónde iba a estar? Bueno, ahí hay alguna discusión en penal, siguiendo alguna doctrina de la corte, que es más civilista que penalista, fuimos al lugar no del hecho, porque el hecho en realidad acá ¿dónde se cometió?, si en realidad está en Internet… Al lugar de los efectos, y la competencia quedó radicada en Trenque Lauquen, que es la cabecera judicial que corresponde a este pueblo.

Y ahí viene la segunda cuestión: ¿qué delito? Que yo creo que de este seminario y de otros eventos académicos en los que participaremos en breve, hay que pensar esto. Primero, si nos alcanzan los delitos que tenemos para este tipo de conductas, o si hay que legislar. Indudablemente hay que legislar. Pero yo reformularía la pregunta. *Okay*, hay que legislar, sería óptimo legislar para tener una figura en la que no haya dudas que esto encuadre. Ahora, de todos modos, esto ocurre, y de lo que tenemos, ¿algo sirve? Bueno, en nuestro caso, "por suerte" —si es que se puede decir que hubo suerte en algo de todo lo que les voy a contar— teníamos la extorsión[5]. Entonces la extorsión es un delito tradicional que no requiere demasiada explicación ni demasiada interpretación. Hay demasiada, acá había claramente una extorsión por chantaje y esto estaba, era probable, digamos.

[5] Artículo 168 del Código Penal: "Será reprimido con reclusión o prisión de cinco a diez años, el que con intimidación o simulando autoridad pública o falsa orden de la misma, obligue a otro a entregar, enviar, depositar o poner a su disposición o a la de un tercero, cosas, dinero o documentos que produzcan efectos jurídicos. Incurrirá en la misma pena el que por los mismos medios o con violencia, obligue a otro a suscribir o destruir documentos de obligación o de crédito".

Artículo 169 del Código Penal: "Será reprimido con prisión o reclusión de tres a ocho años, el que, por amenaza de imputaciones contra el honor o de violación de secretos, cometiere alguno de los hechos expresados en el artículo precedente".

Pero, de todos modos, en el caso nuestro, nosotros avanzamos imputando también el delito de manipulación ilegítima de los datos personales —artículo 157 bis del Código Penal—, que ahí teníamos alguna duda sobre si era de acción pública o privada en aquel momento. A principios de 2013 presentamos la querella penal. Y también vean ustedes cómo uno tiene que intentar "forzar" a veces figuras, o ver de qué manera encausar las pretensiones. También imputamos defraudación de los derechos de propiedad intelectual, porque, vean, dijimos "esto es una obra para la ley de propiedad intelectual", con independencia de las ideas que podamos tener al respecto, y la ley de propiedad intelectual tiene un tipo penal específico, y muy abierto, y muy genérico, digamos, en este sentido. Con lo cual también imputamos eso.

Tuvimos que dejar afuera otros delitos informáticos, como el del artículo 153 bis del Código Penal, la publicación indebida del 155 artículo del Código Penal y las injurias, porque en realidad eso es una acción privada y en la provincia de Buenos Aires, donde esto tramitaba, eso no generaba un riesgo de desdoblar las causas, o sea que se hicieran dos causas y que después la cuestión no avanzara bien, terminar trabados procesalmente. Con lo cual fuimos por la de acción pública.

Como les decía, en nuestro caso tuvimos suerte de que todos los funcionarios intervinientes, no sé si porque es en la provincia, estaban a quinientos kilómetros, teníamos miedo de que fuera algo que los sobrepasara en un punto porque en Capital Federal hay fiscalías especializadas, teníamos más tecnología. Allá no, esto era una cosa novedosa. No, todos los funcionarios que intervinieron en la causa penal, absolutamente todos se consubstanciaron, dieron lo mejor de sí para que llegáramos adonde les voy a contar que llegamos.

La prueba. Con la prueba había un problema, ¿cuál era el problema? El problema era que el primer vector, cuando se sube un video a Internet, alguien lo sube indudablemente a un lugar. Luego de ese lugar, se reproduce en otros lugares, lo baja gente y lo vuelve a subir.

Si uno puede identificar el primer vector, es fácil llegar al autor. Si uno no puede identificar ese primer vector, es casi imposible llegar al autor. Sobre todo en materia de pornografía en Internet, materia sobre la cual, con motivo de este caso, tuvimos que aprender muchísimo, y los

sitios pornográficos de Internet tienen como cuatro o cinco grandes distribuidores de donde los demás después toman. Entonces, si uno lo sube a uno de esos distribuidores, después el contenido se replica automáticamente en otros portales de pornografía, por decirlo de alguna manera.

Acá teníamos que el primer vector que M. había contactado antes de llegar a nosotros; porque después ella les contará cómo llega a nosotros y lo que tarda en llegar a nosotros y el derrotero que ella siente y sufre para llegar a nosotros. Antes de llegar a nosotros ella había contactado a uno de los principales sitios donde este video había sido subido y habían logrado que en uno de esos sitios donde era el vector inicial, bajaran el video. Es decir, ahora estaba en los demás sitios. Entonces nosotros teníamos que asegurarnos la prueba antes de bajarlo de todos lados informáticamente, antes de dar de baja judicialmente el contenido y que lo bajen, teníamos que asegurarlo, con lo cual vean ustedes que acá hay otro elemento de… llamémoslo sufrimiento, porque esa constatación, para hacerla bien y como la hicimos nosotros por lo menos, que entendemos que es como hay que hacerla, hay que hacerla con un escribano, hay que filmar el video, tenerlo nuevamente constatado y todo eso, la víctima tiene que estar nuevamente viendo su video, adelante de otras personas, abogados que están mirando ahí, y la verdad que no es nada agradable todo eso.

Bueno, en este caso, como les decía, fue saliendo todo bastante bien, parece una cosa insólita, se alinearon todos los planetas. Y ese primer vector donde se subió el video por primera vez, lo contactamos por correo electrónico al administrador del sitio, que es un sitio en Inglaterra, y el administrador nos dijo por correo electrónico que el video había sido borrado pero que ellos tenían un *backup* de todo. Y que en ese *backup* figuraba, entre otras cosas, la IP de subida del video. Y que si él recibía un *mail* de un policía o de un funcionario judicial de la Argentina, por *mail* le mandaba toda la información. Y le abría un *backdoor* al video. Todo le dejaba. Dejaba bajar el video para que lo constaten y además le daba la información de la IP de subida. Entonces le requerimos eso a la fiscalía, y la fiscalía accedió, y cuando mandó ese correo electrónico pidiendo la información, y le mandaron la información, y le permitieron acceder al video y demás, la IP de subida era la IP de la casa del imputado. Con lo cual, ya está, desde el punto de vista de la cuestión penal, venía todo perfecto.

El imputado vive en San Isidro. Esto fue, les recuerdo, en 2013 cuando iniciamos la causa, debe hacer sido, febrero, marzo de 2013. En diciembre de 2013 lo citan a lo que sería la indagatoria al imputado. En agosto 2014 se termina la etapa de investigación, la fiscalía requiere la elevación a juicio por delito. Acá, vean esto, a pesar de todo nuestro esfuerzo argumentativo de imputar a otras figuras penales, acá lo que prevaleció fue la extorsión por chantaje, porque estaba acreditada, estaban los SMS en la causa, la prueba fue muy abundante, y de la prueba surgía claramente la extorsión. Con lo cual, acá no era necesario forzar ninguna figura. Extorsión por chantaje, elevación a juicio por extorsión por chantaje.

En ese contexto —y acá es donde empieza, si se quiere, el sufrimiento producto de la permisividad del sistema judicial frente a quienes cometen este tipo de actos— se celebra una audiencia preliminar antes de la elevación a juicio donde el imputado ofrece o requiere la *probation*. Él dice: "Bueno, está bien, ya está, dos mil pesos y no sé qué, terminamos, labores comunitarias".

El fiscal y nosotros por la querella nos opusimos. En nuestro caso, aduciendo que se trataba de un caso de violencia de género citando la Convención de Belém do Pará y el caso "Góngora" de la Corte Suprema de Justicia de la Nación, argumentando que por la forma en que se había dado esto, no era solamente subir un video, era subir un video, las cosas que él puso debajo del video, "contadora *hot*, etcétera, etcétera, etcétera", un montón de cuestiones que si bien no estaba el nombre de ella —no estaba el nombre— sí estaban elementos que permitían llegar, y la cosificación que generó de ella, entendíamos nosotros que estábamos ante un caso de violencia de género, y que por lo tanto no admitía la *probation*.

Por supuesto que el tribunal de Trenque Lauquen estuvo de acuerdo[6] y esto generó que el imputado interponga recurso de casación, y el expediente se fue bien, con la plena prueba que teníamos. Esto quiero que lo tengan claro, un expediente donde era de manual toda la prueba: la IP, estaba todo perfecto. El 27 de diciembre de 2013 teníamos todo perfecto. Se interpone un recurso de casación. En febrero de 2016, la Sala 2 de

[6] Ver texto completo del fallo publicado en *LL* 2016-C-123.

Casación de La Plata declara inadmisible el recurso. Estamos en febrero de 2016. En ese momento, se profuga el imputado hasta agosto de 2017. En agosto de 2017 lo detienen, lo llevan, lo notifican y accede a un juicio abreviado. Juicio abreviado que tiene sentencia el 28 de septiembre, cuya condena es de tres años en suspenso. Ahora, semanas. En su momento lo hablamos con M. porque cada cosa que iba pasando, si bien no era necesario, el fiscal que actúa en la causa nos llamó antes de acordar lo del juicio abreviado, nos llamó y nos dijo: "¿Qué opinan ustedes?". Aunque no requería de nuestro consentimiento, lo hizo, porque quería ir paso a paso con nosotros. Perfecto. Juicio abreviado, tres años de condena en suspenso, ahora el imputado interpuso recurso de casación, con lo cual hoy el expediente está nuevamente en viaje a La Plata. Y esto estamos a, digamos 2017, noviembre de 2017, será un caso que en, no sé, 2018, mediados de 2018 tendremos alguna novedad. Pero un caso en el cual desde el punto de vista jurídico, probatorio, todo está terminado hace tiempo en esta causa penal.

En el ínterin hubo ramificaciones que en este caso fueron tremendamente dolorosas y tremendamente dañosas, tanto o más que lo original, como por ejemplo que cuando al imputado lo llaman a indagatoria, después de que lo llaman a indagatoria, el video que ya no estaba en Internet, o prácticamente no estaba, se vuelve a viralizar. Y se viraliza de un modo muy particular. Esto no está probado en la causa porque esta segunda viralización, si la hubiéramos perseguido en la causa, habríamos detenido todo el proceso.

Entonces decidimos no perseguir esta segunda. No tengo prueba para decir que fue él, pero, oh casualidad, justo cuando lo está, después de indagarlo, aparece de vuelta el video, pero tengo que resaltar algo especial: ¿cómo aparece el video? No sale con el nombre de la víctima. Dice: "Video porno de Soledad Fandiño". Soledad Fandiño es, para quienes no lo sepan, una modelo muy conocida. Entonces, cuando ya parecía que estaba todo terminado en la causa penal —estábamos bastante avanzados, es decir, 2013 o 2014—, un día me llama M.[7] llorando por la tarde y me dice: "Darío, estoy en la televisión en el programa de Del Moro, de vuelta". Ya el

[7] El nombre de la víctima está anonimizado a su pedido.

video estaba bajado de la web. ¿Por qué? Porque se hizo *trending topic* mundial en Twitter el video porno de Fandiño cuando volvió a salir. Entonces hubo que hacer nuevamente toda una serie de cuestiones que ya tenían que ver con bajar el video, no tanto con esta causa penal sino con bajar el video de Internet, lo cual volvimos a hacer, pero vean todo este íter de sufrimiento, en una causa que avanzó bien, en la que se pudo probar todo, en la que los funcionarios judiciales que actuaron, actuaron bien.

Me consta que absolutamente todos estaban preocupados por la causa, porque se produjera la prueba, salvo el allanamiento a la casa del imputado, que lo pedimos en más de una oportunidad y no nos lo dieron, el resto de las medidas probatorias se hicieron todas. Accedieron a mandar un *mail* en inglés al sitio de pornografía para que les mande, todo perfecto, y aún así al día de hoy tenemos un condenado pero sin condena firme. Todavía ni vimos el recurso de casación porque esto fue hace unos días, con lo cual no sabemos ni siquiera qué es lo que está impugnando en ese recurso, pero bueno, o sea, si solamente la condena o algo más, pero bueno, lo veremos. Pero el punto es, entonces, que el fenómeno este es bastante complejo, y acá sumo lo que decían antes en el panel: es mucho más complejo que la viralización de una foto o de un video o lo que fuera.

Yo lo que quiero transmitirles como cuestión positiva, como abogado que hace tecnología, es que por lo menos en nuestro caso se pudo lograr avanzar. Con mucho esfuerzo, y con mucho esfuerzo de nuestro lado porque las medidas probatorias las planteábamos todas nosotros, lo que ocurre es que tuvimos receptividad, pero el punto es que el esfuerzo también lo tenemos que hacer nosotros. También nosotros nos tenemos que capacitar para poder ir y pararnos en un expediente y plantear estas medidas. También eso es una responsabilidad que tenemos que asumir los que llevamos estos temas de tecnología, digamos, de conocer la tecnología.

Pero, bueno, hasta acá mi visión. Quiero que M. les cuente cómo lo vivió ella a título personal.

M.: Bueno, qué tal. Un poquito más o menos Darío ya comentó. Perdón si me quiebro pero realmente me iba acordando de todo y me estoy poniendo muy mal. Como dice él, yo ya venía con amenazas en una relación. Ya me ve-

nía amenazando con que iba a sacar el video, y uno queda en un estado donde yo no podía, no sabía si le tenés que hacer caso, si tratarlo bien, si tratarlo mal, o sea, es difícil porque uno a veces dice de afuera "¿Y por qué le hiciste caso?", "¿Y por qué no?". No sabés, lo único que querés es calmar la fiera.

Igualmente yo ahí, cuando él me venía amenazando, yo me voy a la Comisaría de la Mujer y presento una denuncia diciendo que me está amenazando con sacar un video. Le notifican todo, igual lo saca. Y lo saca. Previamente también me empieza a extorsionar, le pago, y lo saca el día de mi cumpleaños, que fue en diciembre. Y bueno, y a partir de ahí yo ya a la noche empecé a ver cosas raras porque me llegaban muchas solicitudes en Facebook y de otros lados, de Australia, no sé de dónde, bueno. Digo: "Acá pasó algo, y acá atrás está Santiago".

Al otro día me llama una amiga diciéndome que ya lo tenía todo el pueblo, ya se estaba mirando el video, y tal vez quien es de un pueblo puede entender un poco más, cuando son pocos habitantes, lo que significa en un pueblo. Es decir, en ese momento sentís que se te viene el mundo abajo. Tenía una nena chiquita, mis viejos, mi familia, yo que sentía… me afectó en lo laboral, me afectó en lo personal, y mi familia, que también en su momento como que se enojaron conmigo porque en ese momento es como "¿Qué hiciste?", o sea, te empiezan a atacar. Además después comentarios, mujeres, o sea, porque hacer leña del árbol caído es fácil y en los pueblos es así, generaba mucho morbo el tema de una profesional, yo también tengo un estudio, un video porno, todo el mundo mirando, era tema de todo. Tema de la calle, tema del negocio, tema de tema, tema y tema.

Bueno, ahí lo que pude hacer al otro día con un amigo de mi hermana que está acá y que es licenciado en informática, dije: "¿Dónde lo subió? Ayudame a bajarlo, por favor". No sé ni cómo lo hice porque no podía pensar. Bueno, ahí sí empiezo a ver que estaba en todos sitios del exterior. Y dije "Sí", como yo sabía que él estudiaba informática, "no es tonto, no lo subió tal vez en Argentina, que tal vez es más fácil identificar una IP o algo", afuera en el exterior, digo, cómo, o sea, a quién.

Igualmente, de muchos sitios me respondieron y después dije "Yo no me puedo quedar así", y ahí ya digo "Tengo que contactar a algún abogado", y ahí dije: "¿A quién?". Porque un abogado, en el pueblo creo

que no hay ni penalista, pero un abogado, digo, ¿qué?, ¿a quién? Porque tiene que saber de informática, me tiene quedar bola. Yo no me puedo quedar de brazos cruzados y además, sabiendo que es un tema complicado y no todo el mundo sabe. Yo creo que ni sabía que había abogados especialistas en informática.

Bueno, este chico que me estaba ayudando a bajar los videos me comenta de Darío, me da un *mail*, que lo había tenido como profesor, y le escribo. Y ahí es cuando lo contacto. Y bueno, me reúno con ellos y ahí les explico. En realidad, yo necesitaba decir "Bueno, algo tengo que hacer, no me puedo quedar de brazos cruzados y que se salga con la suya", o sea, me sentía muy mal. Después, si no llega a nada, lo intenté.

Cuando me junté con ellos fue cuando sentí un poco de decir, bueno, alguien que me puede dar una mano, porque es difícil, digamos, y además me sentía sola porque mi familia estaba muy mal, no me podían dar tal vez la contención que yo necesitaba, ellos estaban mal, porque a ellos también les afectaba. Les afectaba su imagen, o sea, afecta a toda la familia. Y bueno, ahí es cuando lo comenté y Darío me dice: "Sí, vamos a tomar tu caso". A partir de ahí comenzó, dije "Bueno, tengo un soporte, tengo un sostén", y fuimos para adelante.

La verdad que en estos casos una la pasa muy mal. Voy recordando, o sea, es difícil explicar, pero realmente lo padecí. Porque hubo momentos donde a mí Santiago me decía: "Te vas a tener que ir del pueblo, en las peñas todo el mundo va a ver tu video". Y yo digo "Sí…", no sé si iba a tolerar eso. Empecé, no quería salir de mi casa, tratamiento psicológico, salís a la calle y todo el mundo, nos conocemos todos, o sea, todo el mundo te mira, habla de vos, en general la mayoría habla mal. Sentís apoyo de otra gente, pero me costó mucho. Me costó mucho volver a tener una vida normal para lo que era mi normalidad. Y no sé.

Fuimos avanzando y las cosas se fueron dando muy bien, pero genera muchísimo estrés. Yo además recibía algún… les comentaba a ellos también que hoy alguien me dice "Necesito hablar con vos", y yo ya tengo miedo porque cada vez que alguien me decía "M. , podés hablar", era que algo había sucedido, que el video estaba de nuevo, o esto de Fandiño, o sea, siempre pasaba algo nuevo en todos estos años.

Entonces uno no deja de estar tranquilo y hoy me pasa. Alguien me dice "Tengo que hablar con vos" y digo "Ay, no, ¿qué pasó?". Cuando no, no sé qué, bueno, cualquier cosa, y ahí recién me alivio. Pero, bueno, ojalá que se pueda seguir avanzando con estos temas y hacer algo. Este es un minirresumen …

Marina Benítez Demtschenko: Me gustaría acotar algo cortito, porque si bien nuestras historias tienen muchos puntos en común, hay algo que… estaba anotando cosas… Si bien el tiempo es cortito también, pero con la exposición de esto y la visibilización de la violencia de género virtual, me parece súper importante que no dejemos de tener presente que no se intenta lograr que las mujeres o las víctimas no ejerciten su libertad de expresión por el temor de lo que puede llegar a pasar después con videos y con fotos, porque un conocido me dijo "Al fin de cuentas, esto es la pollerita corta 2.0. Como sabés que puede llegar a pasar, no lo hagas más", y en realidad es parte de nuestra libertad de expresión, es parte del ejercicio de una libertad sexual distinta, que tiene que ver con el uso de las nuevas tecnologías. Estamos en nuestro absoluto derecho de disfrutar de nuestra imagen, de disfrutar de nuestra sexualidad en ese aspecto, y por el hecho de que haya un riesgo o que haya un agresor, no debemos coartarla, y sí estoy totalmente de acuerdo en que el mensaje sea otro: el agresor. Basta de hablar de la víctima, y basta de ponernos a nosotras en cuestionamiento todo el tiempo. Porque me imagino que te habrá pasado, como a mí, el "para qué te sacaste las fotos, para qué filmaste el video, vos no tendrías que haber confiado en él".

Entonces, ¿cuál es la situación de riesgo en la que una se termina poniendo? ¿Confiar en el otro? No, acá tenemos que hacer hincapié en donde se tiene que hacer, y es en el agresor. Por eso también la penalización que, como decía el doctor, hay distintas herramientas para poder abordar hoy por hoy y litigar y judicializar un caso así, pero la penalización también tiene un efecto disuasivo, y la idea es que el peso de la ley caiga sobre la persona que afecta la confianza de una mujer y que además la pone en un riesgo tal que incluso puede, justamente lesionar su vida, la integridad sexual, física, psicológica, como decía hoy.

Demasiados bienes jurídicos tutelados afectados como para que encima la víctima tenga que cargar con esa cuestión social de "Y bue', vas a pensarlo mejor la próxima vez". No, yo la próxima vez voy a hacer lo mismo, la idea es que no haya más agresores que utilicen esto como una herramienta letal contra nuestra libertad. Básicamente eso quería acotar porque por ahí el mensaje que queda después, o subyacente, es este: "Y bueno, cuidémonos", y no "la pollerita corta 2.0 basta".

M.: Pero igual te termina afectando, lógicamente. Pero una cosa es cómo una lo vive y otra cosa es lo que proponen, porque tenemos derecho a ser libres en todo esto. Opino igual, pero digamos, es difícil después. Y sí, obviamente que es muy difícil, así que bueno, listo, eso.

Pablo A. Palazzi: Les agradecemos a todos por la exposición de este primer panel y vamos a pasar al segundo panel, que cuenta con fiscales. Acordamos que cada uno va a contar los casos en los que intervinieron, que son distintos de los de primer panel. Nuevamente les agradecemos a todos por haber venido, especialmente a las víctimas que contaron casos reales y que sirven de ejemplo para demostrar los daños que provocan estos hechos. Muchas gracias a todos.

Así que les presento el segundo panel de la tarde, integrado por fiscales penales de la Ciudad Autónoma de Buenos Aires, de la nación y de la provincia de Córdoba.

En primer lugar, les presento a la doctora Daniela Dupuy, que es la fiscal de delitos informáticos de la Ciudad de Buenos Aires, que aparte fue la primera unidad especializada que se creó en el país. En segundo lugar vamos a oír al doctor Gustavo Dalma, que es fiscal en la provincia de Córdoba. Finalmente expondrá el doctor Horacio Azzolin, que es fiscal federal de delitos informáticos en el Ministerio Público Fiscal de la Nación. Los tres nos van a contar los casos que tuvieron y cómo los fueron resolviendo. Gracias.

Daniela Dupuy: Bueno, buenas tardes a todos, muchísimas gracias por la invitación. Voy a tratar de respetar el tiempo y ser lo más breve posible aunque tengo muchas cosas para contarles.

Trabajo en el ámbito de la Ciudad de Buenos Aires, soy fiscal penal. Me formé en la justicia federal penal y hace cinco años que me desempeño como fiscal especializada en cibercrimen.

La Ciudad de Buenos Aires tiene un sistema acusatorio, un sistema en el que los fiscales recibimos los casos, los investigamos y somos quienes los llevamos a juicio. Claro que en el área de cibercrimen tenemos hoy por hoy muchísimos casos. El ochenta y cinco por ciento son casos de ciberacoso a menores y a mayores. Pero lo más importante es que tenemos fiscalías especializadas en violencia doméstica y en cibercrimen.

La Ciudad de Buenos Aires comenzó con una sola fiscalía especializada, y como la cantidad de casos que ingresaban era realmente escandalosa, hoy hay diez fiscalías especializadas. Equipos fiscales que se dedican a investigar todas las denuncias que llegan en las que las mujeres se encuentran afectadas, ya sea por relaciones intrafamiliares, relaciones con sus parejas y demás.

Los fiscales no trabajan solos sino junto con su equipo especializado, formado, que estudia para investigar y llevar estos casos a juicios con eficientes resultados. Trabajan también con un equipo multidisciplinario, un equipo en el que psicólogos, psiquiatras, asistentes sociales, son los que nos ayudan a llevar adelante todos los casos.

La realidad debo decir que, hoy por hoy, por el avance de las nuevas modalidades delictivas, hay casos en los que nos cruzamos con la fiscalía especializada de cibercrimen. ¿Por qué? En la problemática específica de *revenge porn*, por ejemplo, podemos hablarlo y discutirlo en dos ámbitos. En un ámbito en el que el mayor es el autor y la víctima es la mayor, por lo general, y en otro ámbito donde el mayor es el autor y la víctima es el menor de edad. O, peor aún, cuando el autor es menor de edad y la víctima también es menor de edad (*sexting*), pero no dejan de tener una similitud muy grande con la publicación de imágenes que se tomaron con la anuencia de la víctima pero finalmente son publicadas sin su autorización, con todo lo que implica esto para las víctimas menores de edad.

Hoy estamos a la espera de que se legisle la figura del *revenge porn*, que ya hay muchísimos esfuerzos y proyectos para que esto se haga y se haga bien, escuchando a las víctimas, escuchando también a quienes investigamos este tipo de casos. Es muy importante que los legisladores escuchen a quienes investigamos este tipo de casos para que sepan de

alguna manera intercambiar ideas de cómo tiene que estar descripto este tipo penal, para que nos den la posibilidad de investigar de una buena manera, de investigar eficientemente, donde no haya lagunas normativas.

La Ciudad de Buenos Aires tiene una figura en el Código Contravencional que es el hostigamiento. Hoy, y hasta tanto se legisle el *revenge porn*, cuando nos llegan estas conductas, son encuadradas en la figura contravencional. Así y todo, con el hostigamiento podemos llevar adelante casos en forma rápida, podemos llevar a juicio estos casos. ¿Por qué digo llevar a juicio oral? Institucionalmente tenemos una línea de política criminal con una clara perspectiva de género, y nos prohíben a los fiscales adoptar vías alternativas de solución de conflicto (suspensión de juicio a prueba, mediación) en casos de violencia doméstica. No podemos, más allá de que en algunas oportunidades consideremos que se brindaría una mejor solución si pedimos, por ejemplo, una exclusión del hogar, pues la víctima va a vivir mucho más tranquila y además logramos que ya no se acerque más a ella y demás. Quizás esta sea la solución más eficaz para la tranquilidad de la víctima que la persecución penal y la concurrencia al juicio, con todo lo que ello implica para la víctima, porque es cierto que la víctima tiene que participar de cada uno de los actos procesales. En buena hora.

Cuando yo trabajaba en la justicia federal, la víctima no existía. La víctima iba primero a denunciar a la comisaría, después iba al juzgado, el juzgado no lo escuchaba, no entendía qué pasaba, después iba al otro juzgado, y se declaraba incompetente, y después ante el escribiente tenía que describir todo lo que pasaba. Había una revictimización permanente. Hoy el papel de la víctima empieza a ser tenido en cuenta, cuidado, participativo.

Y sí, a la víctima la necesitamos para comprobar el hecho. Necesitamos que la víctima nos diga, nos cuente, y quizás una vez, y quizás en el juicio oral.

En los casos de violencia doméstica —la mayor cantidad de estos casos—, la prueba vital es la víctima. Porque muchas veces no hay testigos, les diría que en un noventa por ciento de los casos no hay testigos. Son testigos de contexto.

Entonces, la declaración de la víctima, el abordaje de la víctima, debe hacerse profesionalmente, pues su información será muy valiosa.

Lo escuchaba a Darío que hablaba sobre "la capacitación de los actores en esta materia". La capacitación de los fiscales, la capacitación de los jueces, la capacitación de los abogados es fundamental. En el área de cibercrimen, litigo todos los días porque cantidad importante de casos de cibercrimen (pornografía infantil, *grooming*, ataques de negación de servicio, acceso ilegítimo, hostigamientos).

Si ustedes me preguntan "A ver, por ejemplo, los casos de *grooming*: ¿son mujeres la mayoría?", les tengo que decir que no. Las víctimas se conforman por un cincuenta por ciento mujeres y el otro cincuenta por ciento, niños y varones.

Entonces yo entiendo perfectamente esto de que no les devolvemos en absoluto el sufrimiento, el padecimiento a las víctimas. Cuando ayer finalmente la fiscalía ganó un juicio y el juez condenó al imputado en una investigación llevada a cabo en muy poco tiempo (cuatro meses hasta el juicio oral), salí de la sala con un sentimiento encontrado. Con un sentimiento de alegría, porque fue muy bueno el trabajo del equipo, y con un sentimiento de que a esos chicos no les devolvíamos su salud y su integridad emocional y sexual. Su inmunidad sexual yo no se las devuelvo por más que llegue la condena o no llegue la condena.

Entonces, antes de que llegue a nosotros, aquí hay un eslabón previo donde hay que trabajar, y es en las políticas públicas para prevenir este tipo de modalidades. Las modalidades delictivas a través de Internet, a través de los dispositivos de almacenamiento informático, cada día van a ir aumentando más, más, más y más. Debe trabajarse en la prevención, debe haber políticas públicas. Veo muchas ONG que están trabajando, y está muy bien y aplaudo institucionalmente desde diferentes organismos también que se está trabajando en la prevención. Muchas veces son esfuerzos paralelos que deben recobrar fuerza para que el mensaje llegue a todos. Todos juntos debemos trabajar para que esto realmente tenga un *shock* muy fuerte hacia la sociedad. Información, saber de qué se tratan estas conductas, y saber que te puede pasar.

¿Cómo yo voy a imaginar que mi ex pareja, con quien mantuve una relación íntima durante años, que tuve una hija, esta persona por más bronca que sienta por lo que no fue, puede llegar a viralizar un video íntimo de nosotros, con lo que sabe el mal que me puede llegar a generar? Bueno, sepamos que esto ocurre, que esto es cosa de todos los días, y no

es cosa de todos los días en la Argentina, es cosa de todos los días a nivel internacional, porque ya en todos los países está legislado el *revenge porn*. Nosotros siempre estamos como un poco atrás.

Para terminar, porque esto daría como para discutir y contarles millones de casos que tengo del estilo, creo que hay que tener esperanza y hay que tener fe. Es un momento de transición muy complicada, yo creo que la justicia está dando sus pasos. Algunos ya los dimos, o los estamos dando hace más tiempo, y otros que van en sintonía como para generar un cambio. Para que estos casos realmente tengan una buena resolución, para que se puedan llevar a juicio en forma inmediata, para que se puedan litigar, y para que, bueno, las víctimas al menos tengan esa tranquilidad de que alguien pudo hacer bien su trabajo y que veló de alguna manera por esa situación tan tremenda por la que pasaron durante tanto tiempo.

Gustavo Dalma: Buenas tardes, muchísimas gracias por la invitación. Mi nombre es Gustavo Dalma, soy fiscal de instrucción de la ciudad de Córdoba.

La provincia de Córdoba se rige por un sistema acusatorio donde el fiscal de instrucción lleva adelante la investigación penal preparatoria (en algunos casos la investigación está a cargo del juez de instrucción)[8]. La Sede Capital cuenta con fiscalías especializadas, a los fines de investigar determinados delitos. Así, cuenta con la Fiscalía de Lucha contra el Narcotráfico, la Fiscalía de Delito contra la Integridad Sexual, la Fiscalía de Delitos Complejos, la Fiscalía de Violencia Familiar y la Fiscalía en lo Penal y Económico.

Como secretario de instrucción, cumplí tereas en la Fiscalía de Lucha contra el Narcotráfico, y en el año 2014 asumí como fiscal de instrucción en una fiscalía de número, [como] nosotros llamamos a las fiscalías que no investigan un delito específico.

Al poco tiempo, dos excelentes colaboradoras de la fiscalía, Mariana González y Eliana Muir, me ponen en conocimiento de una causa agregando que estaban muy preocupadas porque no podían avanzar con la investigación.

[8] Código Procesal Penal de la Provincia de Córdoba (Ley N.º 8.123).

Era una causa iniciada en diciembre del año 2009. La denuncia la había realizado una joven (mayor) la cual era oriunda de un pueblo muy chiquito del interior de Córdoba, la cual ahora vivía en la ciudad capital para estudiar arquitectura. Que en aquel año había tomado contacto con una persona a través de Facebook con un nombre que, después supimos, el nombre que decía ser era supuesto. Él se hacía pasar por un hijo de un alto gerente de una empresa de telefonía, y después de lograr la confianza con esta chica le empezó a decir que él podía conseguir los códigos de las tarjetas de crédito para la telefonía celular.

En base a eso le decía: "Bueno, yo te doy los códigos, vos pasame una foto de ropa interior tuya y yo te paso los códigos". Cuando le pasó la primera foto en ropa interior, la empezó a extorsionar diciéndole que él le iba a pasar a todos los contactos si no le seguía pasando fotografías. Le causó mucha conmoción a esta chica. Este sujeto empezó a pedir cada vez más fotos, y cada vez con más desnudez. Luego le empezó a pedir filmaciones con determinadas posturas y determinados actos, y para que publique esas filmaciones en la red de internet, le pedía una seña en particular, es decir, que hiciera un gesto con su mano cuando ella estuviera haciendo lo que le ordenaba. Ante esto, a fines del año 2009 decide hacer la denuncia.

Comenzó la investigación y nos encontramos en ese momento con la traba de que las empresas que prestaban el servicio de internet —era una empresa de telefonía celular— que no informaban el IP del teléfono que se conectaba a la red social, porque las empresas de telefonía celular en ese momento no lo registraban, atento que no se lo exigía el Estado. La investigación se detuvo, pues no se podía saber quién era el emisor de esas amenazas, de esa coerción.

Obviamente, al tomar conocimiento a fines de 2015 y principios del 2016, esto me parecía una cosa extremadamente horrorosa. De todos modos, tenía la esperanza de que ya la cuestión se había calmado. Estamos hablando de hechos ocurridos en el año 2009. Así, les pido a las funcionarias que colaboraban con la investigación que citasen a la víctima, a los fines de que comentase si continuaba siendo coaccionada, amenazada. Ella se presenta a la fiscalía y comenta que todavía la seguía coaccionando, el mismo sujeto la seguía extorsionando. Para sorpresa nuestra, acompaña a la instrucción el respaldo informático de lo relata-

do. Ello fue muy importante, pues la víctima resguardó todas las fotos que enviaba y hacía además un "print" de pantalla de todas las amenazas que él le hacía.

En Córdoba, el Ministerio Público Fiscal cuenta con un órgano auxiliar de carácter profesional técnico-científico que colabora con la administración de justicia en la investigación de los delitos de acción pública, que se denomina Policía Judicial,[9] la cual está integrada por abogados, investigadores y técnicos altamente capacitados para este tipo de situaciones.

Un equipo de Policía Judicial fue convocado y empezamos a trabajar con todos los perfiles del victimario que se comunicaba con la víctima, la cual colaboraba en forma activa. Evidentemente volvemos a tener el mismo escollo, pero por suerte en una de todas las oportunidades, desde el año 2009 hasta principios del 2016, el intruso se había comunicado por un servidor de internet por cable. Una sola vez, una sola de las miles coacciones lo había hecho de este forma, es decir no por el servicio de datos del teléfono celular. Esto nos facilitó las cosas, porque inmediatamente pedimos el IP de origen de la comunicación. Teníamos muchas esperanzas de poder ubicarlos, pero éramos conscientes de que la dirección de IP podía estar en cualquier parte del mundo. Mucha fue nuestra sorpresa cuando el informe ubicó la dirección de IP a cinco cuadras del Palacio de Tribunales, donde nosotros estábamos.

Pero nos enfrentábamos a otro desafío, era un edificio. Los investigadores no podían decir con certeza que el titular de ese IP fuera el autor porque se podían estar conectando a través de wifi, es decir, podía ser cualquier persona de todo el edificio. El equipo de Policía Judicial analizó el perfil de todas las personas que habitaban el edificio y detectaron que había uno que coincidía con el perfil de la persona que estábamos buscando. Así que en agosto del año 2016 solicitamos un allanamiento al señor juez de control para poder ingresar al departamento. Al ingresar lo logramos detener al sujeto justo en el momento cuando estaba conectado a una red social coaccionando a otra chica.

Se logró la detención de este chico, y en la computadora tenía dos mil setecientas sesenta y cinco imágenes y videos, en ochenta y siete carpetas.

[9] Web: www.mpfcordoba.gob.ar.

Tenía clasificada a cada una de las víctimas con un nombre y las dividía a todas en carpetas. Los investigadores por análisis de rostros pudieron determinar que aproximadamente había cuarenta y siete perfiles de víctimas.

Cuando esta causa tomó estado público, la víctima no quiso dar a conocer su verdadera identidad; se la llamaba por un pseudónimo. La causa tomo estado público porque el que quedó detenido era un músico de un grupo de cuarteto de Córdoba, uno de los más conocidos,[10] y obviamente la víctima no quiso dar a conocer su verdadera identidad. Ante la publicidad del hecho, dos personas se presentaron espontáneamente en la fiscalía diciendo que también ellas habían sido víctimas, y de todas las dos mil ochocientas fotos pudieron reconocerse entre ellas. La gran mayoría de las fotografías no eran de cuerpo entero, no aparecía la cara, sino que eran todas de partes íntimas, entonces ellas mismas, las víctimas, pudieron identificar las fotos como propias.

Además de eso, los investigadores con las fotos del perfil lograron identificar a cinco personas más. En total pudieron dar con ocho víctimas.

A partir de ahí, y una vez que esta persona estaba detenida, la imputación originaria fue la de extorsión, dictándose su prisión preventiva. Cabe aclarar que en la provincia de Córdoba es el fiscal de instrucción quien dicta las medidas coercitivas. Entendí en aquella oportunidad que la figura penal que le correspondía el imputado era la de extorsión (artículo 168, párrafo 1 del Código Penal) porque entendía que esas imágenes, que eran propiedad de las víctimas, al ser solicitadas coactivamente, la persona no le pedía absolutamente nada a cambio, eso es lo más difícil, no le pedía suma de dinero ni nada, sino simplemente los coaccionaba para que entreguen las fotos a fines de no publicarla en las redes sociales, pero no en forma general sino en forma particular.

Cuando esta chica al principio se empezó a negar a continuar mandándole las imágenes que le pasaba, él creó un perfil falso y las fotos, el link de las fotos para mostrar, era la víctima desnuda. Y les mandaba invitaciones a todo el grupo de contactos que ella tenía en la red social.

A partir de ahí, accedían a lo que él les pedía, y si no lo hacía les mandaba directamente a los amigos invitaciones con la foto de la víctima

[10] "Imputan a músico de Trulalá por extorsionar mujeres en Facebook", en *Córdoba Times*, 3 de septiembre de 2016 [http://bit.ly/2MSOSBY].

desnuda. A esta chica, al ser de un pueblo extremadamente pequeño, le impactaba muchísimo y continuaba haciendo lo que él le pedía por el tremendo temor que ello le ocasionaba.

De esta extorsión que inicialmente fue imputada esta persona, el abogado defensor se opuso (recurrió la medida coercitiva dictada), fue al juez de control para dirimir la cuestión. El juez, al revisar la medida coercitiva dictada, la mantuvo pero hizo algunas observaciones a la calificación legal. Dentro de las calificaciones legales, él entendía que no se había afectado el patrimonio de la víctima y, al no verse afectado el patrimonio de la víctima, no podía haber extorsión, solo coacción, *pero sí entendía que se había vulnerado la intimidad sexual de la víctima*.

Entonces entendió que, con el accionar del imputado, [este] había ultrajado al pudor de la víctima. Al abrir esta posibilidad, no tenía muchos caminos más allá de remitir las actuaciones al fiscal especial en delito contra la integridad sexual, porque así lo había dicho el juez de control, y como es una resolución superior, cualquier resistencia mía iba a terminar revocándola el mismo juez.

Inmediatamente después de remitir las actuaciones, comenzó a actuar la fiscal de delito contra la integridad sexual. El volumen de la investigación era inmenso, y en estos días [2017], para no excederme en el tiempo, se acaba de confirmar la elevación de la causa a juicio. La persona continúa detenida, todas las medidas que tendieron a revocar la medida coercitiva dictada por el Ministerio Público fueron todas rechazadas hasta la última instancia, y se ha elevado esta causa a juicio por ocho hechos (por ser ocho las víctimas identificadas). Se siguen investigando los otros, pero los delitos fueron coacción calificada continuada, calificada por el anonimato y abuso sexual gravemente ultrajante calificado por el grave daño producido en la salud psíquica de la víctima. Eso es la calificación legal que actualmente tiene, no me voy a explayar en las otras víctimas; había víctimas que cuando empezaron a ser coaccionadas eran menores de edad, así que también se le imputó la producción de pornografía infantil. En conclusión, está imputado por todos los hechos en forma reiterada y hay ocho hechos en concreto, así que, de ser condenado, la pena va a ser extremadamente alta.

En estos momentos está a la espera del juicio pero está confirmada, así que yo creo que a la brevedad se le va a hacer un juicio a esta persona.

Esa es la investigación que nosotros hicimos, eso es lo que quería compartir con ustedes no solo sobre lo dificultoso de estos hechos delictivos, sino también en lo dificultoso que resulta calificar penalmente estos hechos que vulneran distintos bienes jurídicos, conducta esta que no está tipificada aún en nuestro código de forma.

Horacio Azzolin: Buenas tardes a todos y todas, soy Horacio Azzolin. Como dijo Pablo Palazzi, soy fiscal federal. Estoy a cargo de la UFECI, la Unidad Fiscal Especializada en Ciberdelincuencia,[11] que trabaja delitos federales en el interior del país, y en la Capital Federal delitos federales y delitos criminales aún no transferidos a la justicia desde la Ciudad Autónoma de Buenos Aires.

Les quiero contar un poco, de la mano de lo que contaron mis colegas, cuáles son los problemas que yo veo alrededor de este fenómeno, que creo que todos coincidimos en que está creciendo cada vez más.

Yo pensaría en tres ejes, por lo menos, como para que discutamos un poco después, ya que se van a ir tocando durante este encuentro.

Por un lado, el tema de cómo es la mecánica o la dinámica de estos casos en base a los que nos llegan de alguna forma a la UFECI: o por denuncias directas o por consultas de otros fiscales. Por un lado, tenemos como dos grandes escenarios de la difusión de imágenes íntimas: tomadas con consentimiento o sin consentimiento.

Marina nos ha contado casos de imágenes tomadas con consentimiento en el marco de una relación de pareja o de algún tipo de relación, y que luego son de alguna forma utilizadas para cometer delitos. Gustavo Tanús nos contó acá casos de imágenes tomadas bajo coerción y que después son utilizadas para otros fines. Esos son dos de los grandes escenarios que hay.

Tal vez la idea de las imágenes tomadas bajo coerción es una mecánica un poco más antigua y que ya se viene dando en muchos casos. Muchos casos que empiezan con un contacto que podríamos considerar o encuadrar en *grooming*, terminan después derivando en encuentros personales o en la coacción para obtener imágenes y, a partir de estas imágenes, más coerciones. En la fiscalía tuvimos hace unos años un caso de 2008, antes

[11] Web: www.mpf.gob.ar/ufeci.

de la ley de *grooming*, antes de la ley de delitos informáticos; se usaba Messenger en ese momento todavía, donde esa dinámica había estado presente. Me acuerdo de que al imputado le impusieron catorce años de prisión. La UFECI no existía como tal, era un caso más viejo.

Lo que sí estamos viendo ahora, como fenómeno más reciente, es otro tipo de casos más complicados. Esta idea de la difusión de imágenes íntimas que a veces son intercambiadas en el marco de una relación o a veces son tomadas por una persona y accedidas indebidamente por otros.

Entonces esa es otra de las cuestiones que nosotros empezamos a ver y que tratamos de protocolizar en los casos para ver de dónde salieron esas imágenes. Tenemos muchísimos casos de gente que se toma imágenes íntimas que se autosacan, las *selfies*, etcétera, y tenemos casos de intercambios en el marco de relación de parejas que después, truncada o no, son utilizadas, o casos en los cuales son intercambiadas en el marco de supuestas relaciones que en realidad nunca lo fueron sino que eran solamente medios para obtenerlas. Y ahí empezamos a tener problemas de encuadre.

Cuando hay exigencia de dinero, es como que cada vez es más velada y un poco los problemas que contaba Gustavo Tanús acerca de la posibilidad o no de considerarlo una extorsión, que sería la figura más grave y la más seductora para nosotros, los fiscales. Porque la expectativa de pena es enorme, cambia si el imputado llega o no a libertad del proceso, la expectativa de pena es altísima comparada con el resto de los delitos posibles. Lo que estamos viendo es que hay como una sofisticación en el pedido y no hay una exigencia, o a veces es muy difícil encuadrar esa exigencia en lo que puede ser una extorsión o en realidad un chantaje. Eso, por un lado.

Cuando no tenemos presente ese pedido, a veces son solamente puestas esas imágenes en foros. Hemos visto mucha colocación de esas imágenes en foros públicos, en redes sociales, en páginas dedicadas exclusivamente a eso. Ahí lo único que podemos hacer es ver si esas imágenes fueron obtenidas ilegalmente. Y ese es un problema, porque cuando esas imágenes no fueron obtenidas ilegalmente, muy probablemente no tengamos caso para procesar. Sobre eso creo que va a hablar en el último bloque Pablo Palazzi, de las propuestas legislativas.

Cuando a mí me preguntan qué delito habría que reformar del Código Penal, me parece que ese es el principal. Ese es un problema

que nosotros vemos como un drama muy grave para las víctimas, y que hay casos en los cuales no podemos dar una solución efectiva. Así que ese es un tema, las modalidades. Y sobre esas modalidades yo no tengo la libertad de comentar demasiado de algunas investigaciones que tenemos, pero lo que sí les puedo decir es que estamos viendo ya organizaciones criminales que se están dedicando a esto. No son a veces exclusivamente situaciones de individuales que interactúan con una persona o con varias, como el caso que comentó el doctor Tanús; me hace también acordar al caso de Micaela García. No es solamente eso, sino que también estamos viendo organizaciones que se dedican a generar contactos de ese tipo al solo efecto de después extorsionar a sus víctimas. Muchas de esas organizaciones actúan en las redes sociales que usamos todos, que se usan para conseguir pareja o para conseguir algún tipo de encuentro, y muchas de esas organizaciones actúan en plataformas que nunca nosotros nos hubiésemos esperado que las utilicen para eso. Así que ese es un problema mayor. Y estamos viendo casos de organizaciones que atacan, que tienen objetivos en múltiples países, así que es un fenómeno como para ver, porque mueve muchísimo dinero por abajo.

Después, por el otro lado, por lo general no tenemos problema en la localización de los autores de estas maniobras, son más o menos identificables, salvo en hipótesis de sustracción de imágenes, porque o llevé el celular a arreglar, o alguien accedió a mi computadora, o la dejé abierta con la sesión iniciada en un cibercafé o locutorio, etcétera.

Pero sí hay otra cosa, que nosotros tratamos de hacer y se hablaba también en el panel anterior, que es el tema de lograr la supresión de contenidos. Y en ese sentido hemos tenido muchas malas experiencias y muchas buenas también. Estamos trabajando bastante con algunos proveedores. Siempre lo que nos pasa es que tenemos que trabajar con proveedores de afuera, pero estoy empezando a notar que hay cierta sensibilidad de los proveedores acerca de… no sé si la responsabilidad o civil pero sí cierta responsabilidad en que esos contenidos no sean publicados en la página en la medida que alguna autoridad judicial les informe que ese contenido ha sido generado o ha sido compartido sin autorización de la persona que participa de ese contenido, sin consentimiento. Así que hemos tenido muy buenos casos de supresión

de contenidos, incluso en casos que no hemos podido procesar como delitos porque no los podíamos encuadrar en ninguno.

Esa es una medida a tener en cuenta. Me parece que las normas que rigen en Argentina no son lo suficientemente claras para eso, y sobre eso habría que trabajar más fuertemente. A nosotros nos pasa en otros aspectos que tienen que ver con la supresión de contenidos que son de violencia de género. Una cosa es que aplicando las leyes vigentes nosotros podamos intimar a alguien a no difundir imágenes. Si yo sé que el Sujeto A tiene imágenes de la víctima, yo le puedo decir al Sujeto A "Abstenete de hacerlo", puedo hacer una medida cautelar, y hay casos bastante famosos que estuvieron en los programas de chimentos todo el año, que nosotros incluso usamos como para apoyarnos en eso.

Pero cuando el contenido es difundido por NN, ahí es más complicado, y cuando ese contenido hay que ejecutarlo afuera, también es más complicado. Entonces la realidad es que si nosotros tuviésemos normas, un poco más de musculatura legal, tal vez podríamos llegar mucho más rápido, o incluso también la víctima podría llegar mucho más rápido sin depender de nosotros necesariamente. Así que ese es otro tema para tener en cuenta, como para tomar nota.

Y lo tercero, un poco de la mano de lo que dice Daniela Dupuy, es que nosotros siempre llegamos tarde a estos casos. Y la realidad es que muchas veces no sabemos cuál es la mejor forma de pararnos frente a la concientización de los usuarios de Internet.

Hay un aspecto que me parece que es más fácil, que es: la persona que tiene imágenes íntimas en sus dispositivos lo que puede hacer es cuidar esos dispositivos de determinada manera. Los casos que nosotros hemos tenido de acceso ilegítimo es gente que no tenía el doble factor de autenticación, que su contraseña no era robusta, que dejaba las sesiones abiertas. Entonces, con dos o tres cosas, con dos o tres consejos pueden robustecer sus dispositivos y asegurarlos. Yo siempre propongo el mismo ejercicio. Yo asumo que todos acá usan doble factor de autenticación, pero vuelvan a sus casas y pregunten en su grupo de amigos, en la salida del fin de semana, en el asado del fin de semana, en el fulbito del fin de semana, cuántos tienen doble factor. Y les propongo algo más: si ustedes tienen doble factor, háganselo poner a sus amigos.

El otro día un amigo chileno que trabajó en la redacción de la estrategia de ciberseguridad de Chile decía que la ciberseguridad es una responsabilidad compartida. El que sabe, tiene que enseñarla también. Entonces no es solamente que nosotros les mostremos a nuestros amigos que tenemos la aplicación con el verificador de Google, o que tenemos la llavecita de seguridad re *cool* que nos compramos en Amazon. El tema es: tenemos que hacer que los otros lo tengan también. Porque esa es una forma de asegurar nuestros dispositivos, y en definitiva de asegurar nuestra información y también nuestra intimidad.

Me parece que hay un tema más complicado de encarar, y yo sinceramente no sé cómo pararme en esto, que tiene que ver con la difusión consentida de imágenes. He visto muchas campañas de concientización diciendo "No compartas imágenes". Me parece que eso es del siglo XIX. Es una actitud del siglo XIX y de meter miedo, entonces tenemos que ver otra forma de hacerlo, porque si yo quiero hacer de mi sexualidad el intercambio de imágenes, tengo todo el derecho de hacerlo. Entonces no sé si es el lugar correcto pararse diciendo "No compartas imágenes" o "Tapate la cara" o "Poné un emoji". Me parece que no pasa por ese lado, pero no sé por dónde pasa. Sinceramente no sé por dónde pasa y no sabemos cómo comunicarlo. Y ese es un problema también, porque es un problema que nos golpea permanentemente, que nos interpela, que nos interpela en las víctimas, que nos interpela en los casos, que nos interpela la impotencia de no poder procesarlos a veces, nos interpela incluso lo que tardan los órganos legislativos en sancionar las normas que necesitamos. Pero siempre pasa. Y sin embargo es muy difícil saber cómo pararse frente a estos fenómenos.

Me parece que una opción es hacer esto. Yo recién le decía a Pablo Palazzi, antes de que empiece, que qué bueno que un programa como este de la Universidad de San Andrés se siente a trabajar estos temas. En vez de hablar de acceso ilegítimo, *etical hacking*, acceso remoto a dispositivos, que son temas súper interesantes, también ponernos a discutir qué nos pasa como usuarios de Internet, como adultos que queremos tener sexo de la forma en que se nos ocurra, y cuáles son los problemas legales y cuáles son realmente las impotencias que tenemos. Nosotros tampoco tenemos todas las respuestas a todo, y sí somos tan usuarios de Internet

como nuestras víctimas. Entonces me parece que es un tema como, por lo menos para discutir así, para no solaparnos, y también como para pararnos frente a determinadas actitudes. Y una actitud me parece que, por lo menos desde lo sano y me parece que está muy bueno como campaña y como interpelación, es "no compartir".

A todos nos habrán llegado las fotos de Latorre, los audios, o de otros casos conocidos. No los compartamos. Si podemos, incluso, censuremos al que los manda. Me parece que la mejor forma de parar eso es no quedarnos callados frente a lo que pasa, y realmente mostrar que es una práctica no consentida, no solamente compartir sino también no decir nada. Entonces empecemos a levantar la voz y a decir "no compartan también". Me parece que por lo menos es un paso. Cuando vean que nosotros objetamos esa práctica, tal vez por lo menos no nos manden y tal vez generemos conciencia en el otro también. También creo que esa es una responsabilidad compartida.

Bueno, creo que estamos bien de tiempo, así que estamos para ustedes.

Pablo Palazzi: ¿Alguien quiere hacer alguna pregunta?

Pregunta del público: Una para Gustavo y una para el panel en general. Cuando hablabas de que cotejaron el perfil de la persona con los perfiles de la investigación, ¿a qué te referís específicamente? ¿Cuáles eran los puntos de cotejo, si lo podés contar? Y después, al panel en general, una inquietud que, si bien yo no me dedico a temas penales, es algo que me viene rondando y es el tema de cuando vos generás la imagen y vos la enviás, si no se puede aplicar desde el lado de derechos de autor, porque derechos de autor te remite a las penas de la estafa, no sé si se les planteó alguna vez esa estrategia.

Gustavo Dalma: Cuando yo hacía referencia al análisis de los distintos perfiles, porque esta persona tomaba de los perfiles para buscar a las otras víctimas, entonces él tomaba una víctima, por eso la mayoría eran de una sola localidad, porque empezó a coaccionar a las personas que él conocía, tanto así es que una de las víctimas que se presentó espontáneamente a la fiscalía era su novia, es decir, a la misma novia la empezó a extorsionar,

la novia le mandaba, por eso una persona bastante compleja psicológicamente, porque la novia le mandaba… Como él era también de otro pueblo, cuando él viajaba le pedía que le mandara, y al poquito tiempo a la novia le empezaron a llegar coacciones con las fotos diciendo "Tengo estas fotos, empezá a mandarme mas fotos", y era él mismo. Entonces, asustada, le dijo a él: "Mirá, ¿vos le pasaste las fotos a alguien? ¿Cómo puede ser que ya las tenga?". "No, te han hackeado el teléfono, pero hacé lo que a vos te dice porque si no todos tus amigos se van a enterar", y la extorsionaba a la misma novia. Entonces eso es lo que él hacía, es decir, tomaba los distintos perfiles de los amigos para empezar a extorsionar y buscar posibles víctimas. Entonces la gente de Policía Judicial empezó a analizar las fotos con todos los links de todos los perfiles de todos los amigos, que fue una labor extensa y compleja, y así pudieron ubicar solo a cinco víctimas, y siguen trabajando con los otros cuarenta y siete, eso es lo que estuvimos haciendo.

Horacio Azzolin: Nosotros pensamos eso como plan B, la reproducción no autorizada de una obra. En realidad, nunca lo llegamos a usar. Lo planteamos, lo pensamos como posibilidad para suprimir contenido. Pero en realidad lo que nosotros planteamos en los casos donde, a ver, cuando nosotros tenemos que ponernos a trabajar con proveedores del extranjero, lo primero que tenemos que ver es si cuando tocamos timbre abren la puerta. Algunos te contestan, otros no. Los que nos contestaron, cuando les planteamos qué tipo de caso era, suprimieron el contenido directamente. Con lo cual no llegamos a eso. Pero puede ser un argumento. Veíamos alguna dificultad en que estábamos "invisibilizando" el caso real. Era como, si yo hablo de un caso de propiedad intelectual, no es un caso de violencia de género. Entonces ese es el problema. Pero, para plantearlo en países que tienen leyes de protección de propiedad intelectual fuertes, por ejemplo la Unión Europea puede, lo habíamos pensado como posibilidad, no lo usamos nunca.

Daniela Dupuy: El desgaste es tremendo porque todas estas conductas que se nos presentan en el día a día —no solamente esta, muchas otras—, a la hora de subsumirlo en algún tipo penal, se nos empieza a

dificultar, es decir, cuánto tiempo de tu investigación tardaste para hacer una elaboración en base a este tipo penal que no sabemos si en definitiva lo van a condenar por eso. Entonces es realmente desgastante, por eso trabajar mucho a medida que van apareciendo estas nuevas modalidades, dar una respuesta. También parte de una discusión es decir "Adecuamos lo que ya está o vamos tipificando todas y cada una de las modalidades que aparecen". España tipifica absolutamente todo. Bueno, es una discusión, algunos están a favor, otros están en contra. El Derecho Penal como última *ratio*. Muchas veces hay temas, en España hay discusiones muy importantes con este tema del *revenge porn*, si el que consintió, si el que no consintió por qué mandó la imagen, por qué no lo hizo, quién es el autor, si es el primero que difunde, qué pasa con el resto que las reciben y siguen difundiendo, la responsabilidad les alcanza a esos o simplemente se queda en el primer emisor… Bueno, hay una serie de cuestiones que hay que discutir, y lamentablemente —a lo mejor Pablo Palazzi está de acuerdo conmigo— tenemos legisladores que si bien muchos están, digamos, con una muy buena predisposición para escucharnos y escuchar a todos los que presentan diferentes proyectos, falta hilar más fino. Falta esa capacitación, falta eso de meternos en la materia para entender de lo que estamos hablando.

Entonces, muchas veces, la labor de los fiscales, de los jueces, se nos torna muy complicada. Acá tenemos a un juez de la ciudad que sabe de lo que estamos hablando, el doctor Pablo Casas, y bueno, que trabajamos mucho este tipo de casos, y realmente no solo son muy dificultosas las investigaciones, sino en la previa, buscar el tipo penal, subsumirlo en el tipo penal para correctamente cada una de las conductas analizarlas a la luz de la prueba y subsumirlo en cada elemento normativo del tipo. Hablemos del *grooming*, no vamos a hablar ahora, pero el *grooming* es un tipo penal que a mi entender quedó muy mal redactado, pero eso lo puedo advertir una vez que estoy investigando y que me doy cuenta de que no puedo cumplir con lo que la ley me pide, a pesar de tener un caso fuerte.

Nos costó tanto a nosotros calificar la conducta, y es tan importante enmarcarlo en un tipo penal porque ese es el norte de la investigación, entonces todo lo que nosotros podamos requerir al juez de control, que tiene que dar la autorización, tenemos que decir el "para qué". Entonces,

si no le decíamos qué es lo que estamos nosotros investigando, cuál es la hipótesis delictiva que nosotros estamos tratando de defender o tratando de demostrar, el juez de control, que es el que nos habilita distintos procedimientos, yo no le puedo decir "Esto es gravísimo, tenemos que ir para varios lados", tengo que mostrarle el camino y tengo que encuadrarlo en un tipo legal, que eso fue toda una discusión.

Creo que son muchos esfuerzos, en esta problemática específica que hoy estamos discutiendo, pero en todo lo que incluye el cibercrimen, como todas las conductas que se cometen a través de Internet. Es, por empezar, un triple esfuerzo. El de la prevención, el de concientizar a la sociedad, el de concientizar y formar a los menores, a los mayores para evitar este tipo de conductas, porque yo no quiero que me ingresen tanta cantidad de casos de este tipo. Pero no porque no quiero trabajar, porque amo lo que hago, sino porque me queda, como decía antes, este sabor amargo, más allá de ganar el caso. Los que pierden son las víctimas, entonces, por más que consigamos muchas veces condena los fiscales, no está bueno. Jueces, fiscales y abogados a la altura de las circunstancias, digamos, vamos a litigar y tenemos que estar todos sabiendo de lo que estamos hablando. Si yo le voy a presentar un caso al juez donde tiene que entender toda la cuestión técnica de cómo llegué a esa determinada IP, cómo analicé la información de las fuentes abiertas, bueno, primero tengo que entenderlo yo, tiene que entenderlo mi equipo, el juez tiene que tener un conocimiento medianamente básico para estar abierto a ese entendimiento, y un abogado defensor que lógicamente, para ejercer correctamente el derecho a la defensa que tiene el imputado, estar también al tanto de estas circunstancias.

Y por último aunque no menos importante: la legislación. La legislación penal y la legislación procesal. Tenemos una legislación procesal arcaica. Hay un principio de libertad probatoria que los fiscales, en un ámbito acusatorio como el de Ciudad de Buenos Aires y como en muchas provincias, ya no sabemos más cómo estirar ese principio de libertad probatoria. Vamos, legislemos, hay herramientas probatorias, tecnológicas, que las debemos colocar expresamente en el Código, para que después, lógicamente y con razón la defensa no nos plantee nulidades por prueba a la que llegamos por medios de prueba que no están estipulados en las normas procesa-

les, y ni hablar con el Código Penal. Tenemos la ley de delitos informáticos, pero estas nuevas modalidades que estamos hoy discutiendo, no están. Y en Ciudad de Buenos Aires tenemos el hostigamiento. A ver, sinceramente, ni siquiera está a la altura de las circunstancias tener que llevar un caso a juicio por hostigamiento. La conducta es mucho más grave, merece una pena, merece una sanción penal, después vemos si cuando lo analizamos a la luz de la sistematización de las penas del Código Penal le ponemos cumplimiento efectivo, cumplimiento en suspenso. Pero esto tiene que ser un delito, claramente tiene que ser un delito, no una contravención. Entonces hoy, bueno, nos tomamos de la contravención, el hostigamiento, nos abre un espacio para que podamos insertar estas conductas que el legislador todavía no tipificó. Y ahí estamos, en la lucha, día a día.

Pregunta del público: En términos generales, en el caso de pornografía no consentida físicamente, ¿los casos vienen acompañados de extorsiones y de hostigamiento, o hay muchos casos?

Daniela Dupuy: Los casos que me llegan a mí, porque con Horacio [Azzolin] tenemos dividida la competencia, yo no soy competente en lo que es la extorsión propiamente dicha, entonces si yo tengo comprobada la extorsión, ya ahí tengo que decirle a nación que intervenga. Los casos en donde, bueno, hay simplemente o un acoso virtual, o una publicación de imagen sin consentimiento de la publicación de la difusión pero sí de la toma de esa imagen o de ese video, ahí sí nosotros la seguimos adelante porque muchas veces, cuando no hay extorsión, en el ámbito nacional no hay tipo penal para poner, entonces mínimamente, al menos, hacemos la investigación con el hostigamiento.

Pregunta del público: ¿En general los casos vienen acompañados del hostigamiento?

Daniela Dupuy: Es que lo encuadramos en el hostigamiento, no nos queda otra alternativa que encuadrarlo en el tipo contravencional porque es una situación intimidante, es una situación que acecha a la víctima, entonces decimos, bueno, ¿dónde va? En el hostigamiento.

Pero al menos podemos darle una respuesta a la víctima. A través de una medida alternativa de solución de conflictos, a través de llevar el juicio, investigamos el caso en tiempo y forma, tenemos un Código Procesal Penal que nos dice "Tenés tres meses para investigar el caso a partir de que lo intimaste de los hechos al autor". La verdad es que los tiempos en Ciudad de Buenos Aires, aun en los casos complejos, son tiempos cortos que los fiscales llevamos los casos a juicio, y esto hablo de los casos de violencia doméstica, de las fiscalías especiales de violencia doméstica, de las tres fiscalías en cibercrimen, y hoy la buena noticia que tengo es que los jueces empiezan a jugar en el buen sentido. Empiezan a entender de qué se trata esta dinámica y esta necesidad que todos tenemos de que, cada uno desde su rol, adaptarnos a esta nueva dinámica. Todos, seguramente jueces, fiscales, defensores, nos educamos en un sistema diferente. Hoy por hoy la sociedad nos pide que son nuestros clientes a quienes les tenemos que dar una respuesta, hoy nos piden que estemos a la altura de las circunstancias y que les demos una respuesta en tiempo y forma, y juramos para eso. Nuestra obligación es realmente esa, poder dar una buena respuesta a todos. A veces se puede y otras veces no.

Horacio Azzolin: Eso, lo que decía Daniela [Dupuy], frente a un caso, vos empezás a tratar de segmentar, tenés pedido de plata o no tenés pedido de plata. Y cuando no tenés pedido de plata, empezás a ver. Las imágenes se obtuvieron con consentimiento, no tenés un acceso ilegítimo a un dispositivo, no tenés una interrupción de comunicación electrónica, la única posibilidad es la que dice Daniela [Dupuy], el hostigamiento. Si no, vas siempre a la mejor figura. El problema que tenemos es este: a veces los pedidos son sutiles, a veces son muy expresos. Ayer tuvimos un caso de un varón que le pasó lo mismo. Cayó de una red que estaba operando en Ecuador ahora, que contacta aleatoriamente a la gente de todos los países. Y ahí el pedido de dinero es expreso, es clarísimo, pero hay casos que son mucho más sutiles. No sé qué va a pasar. Entonces, ¿qué hacés? Buscás la forma. Los casos que nosotros tenemos, de todos los casos que nosotros tuvimos, la mitad no se pedía dinero, fueron a Ciudad de Buenos Aires. Y la otra mitad se pedía dinero. No sé si te puedo dar un patrón concreto sobre eso.

En el caso que nosotros tuvimos no se pedía dinero, él simplemente hacía eso por una cuestión, coleccionaba en una forma extremadamente ordenada. Para nosotros estuvo bueno porque no tuvimos que dividir los perfiles, pero en cada carpeta guardaba uno, y después de esos cuarenta y siete perfiles teníamos que ubicar sí o sí a la víctima para saber si esas fotografías que aparecen ahí eran consentidas o no. Porque nosotros teníamos que contactar necesariamente a las víctimas para que nos digan si fueron bajo coacción o no.

Daniela Dupuy: Hay otra problemática también que va de la mano de todo esto que vamos discutiendo: el tema de los menores de edad. Cuando las víctimas son menores de edad. Y acá hay un escenario que es muy común hoy. Un chico de dieciocho años con una de dieciséis, que mantienen una relación, que se sacan fotos, que hoy es muy común entre adultos pero entre chicos también, se sacan fotos llevando a cabo una actividad sexual, la viralizan entre el grupo de amigos. Aquí lógicamente las denuncias que tenemos de esto siempre vienen acompañadas de los papás de la menor, porque siempre las víctimas somos las mujeres, es la menor, porque al varón no sé si le interesa tanto a los dieciséis, diecisiete años que le publiquen este tipo de fotografías, pero lo cierto es que vienen siempre los padres de las menores de edad trayendo este problema, que se viralizó una foto de su hija de dieciséis, quince, catorce años, está llevando a cabo una actividad sexual y todo el mundo tiene ese video. Lo tiene el colegio, lo tiene el club donde la nena juega al hockey. Ahora acá tenemos otra problemática porque vamos nada más al ejemplo del mayor, dieciocho, diecinueve años con la menor de dieciséis, que siguen siendo pareja, no hay venganza acá, se viralizó porque es una costumbre. Bueno, ojo, porque acá son imágenes que podrían ser imágenes de pornografía infantil por ser menores de edad, entonces el autor estaría cometiendo el delito de distribución de pornografía infantil, o facilitación, o depende del medio por el que lo haya compartido. Entonces acá empiezan otras cosas en juego.

En los casos que nosotros tenemos, por ejemplo, el consentimiento de la víctima siempre fue tapado por la decisión de los padres de llevar a cabo la denuncia. Es decir, una cámara Gesell que hicimos justamente

yendo a esto de qué pasa con el consentimiento de la víctima de dieciséis años, de diecisiete años, donde este tipo de relaciones ya empiezan a ser un poco más consentidas, lo que no quiero es que lo difundas, lo que quizás me puede llegar a mí a perjudicar es la difusión. O no. En España hay un estudio que dice que el 48% de los jóvenes naturalizan absolutamente estas prácticas, y que están consentidas estas situaciones con las menores, que no se encuentran afectadas por esto.

Pero, en los casos concretos que hemos tenidos nosotros, la víctima en un caso dijo "A mí no me parecía tan grave hasta que mis padres me hicieron tomar conciencia de que había que denunciarlo, porque era un delito", y demás. Pero bueno, después hay de todo, porque hay casos en los que la menor pudo haber consentido, no le pudo haber molestado la publicación, pero hay otros casos, por ejemplo un caso que hemos tenido que comenzó con un *grooming*, con un acoso y era un profesor de piano de una academia a una alumna de dieciséis años, y empezó digamos una relación de ida y vuelta consentida por la menor, con fotos que ella le mandaba, con videos que ella le mandaba. Han tenido un encuentro, tenían un tipo de relación, pero cuando la menor quiso salir del juego, ahí él no la dejó. ¿Y cómo no la dejó? Diciéndole de alguna manera: "Bueno, mirá, si vos no me mandás más fotografías, mirá cómo te publico este video", y ahí la chica se desesperó y ahí acudió a sus padres y formalizaron la denuncia.

Tenemos de todo. Sí se puede subsumir en algún tipo penal perfectamente. Otros se pueden subsumir pero el tipo penal es desastroso. Y en otros básicamente no tenemos tipo penal para trabajar. Todas las herramientas sí para investigar. En Ciudad de Buenos Aires tenemos un cuerpo de investigaciones judiciales que trabaja profundamente estos temas codo a codo con los fiscales.

Ayer tuvimos esta audiencia que les cuento; la de ayer fue otra que tuve de prisión preventiva. En esa audiencia, era de un pedófilo, el cuerpo de investigaciones judiciales nos iba mandando online la prueba, porque uno de mis principales fundamentos para que la jueza lo dejara preso hasta el juicio —después vemos qué pasa— era justamente que estábamos terminando de analizar todos los dispositivos de almacenamiento informático con el cuerpo de investigaciones. Una de las muestras que le

dio la fiscalía de que era cierto esto era que el cuerpo de investigaciones nos iba mandando online la nueva prueba que iba recolectando, aparecían nuevos menores afectados por esa persona que estaba ahí, esposada.

Entonces la defensa dice "Perdón, es un hecho nuevo, yo no lo voy a admitir bajo ningún punto de vista", y la jueza dijo "Perdón, yo soy muy respetuosa del principio de libertad probatoria, tanto de la defensa como de la fiscalía, y entiendo que los jueces debemos *aggiornarnos* y adaptarnos a los avances de las nuevas tecnologías, y si la fiscal en estos momentos está queriendo incorporar una prueba en forma virtual, en forma online, para que yo pueda decidir acerca de la medida cautelar que me está pidiendo la fiscal, bienvenida sea". Así que hicimos un print de pantalla y se lo mandamos. Igual eso no le cambió su decisión porque ya había muchísima prueba que habíamos trabajado en cuatro días. En cuatro días. Por eso digo, no hay que perder las esperanzas, creo que si bien hay ámbitos judiciales donde les cuesta todavía muchísimo *aggiornarse* y estar realmente, tener las herramientas como para poder dar una buena respuesta, hay otros que estamos con mucho esfuerzo y mucha responsabilidad, poniéndonos realmente a la altura de las circunstancias para poder darle una respuesta a la sociedad.

Pablo A. Palazzi: Bienvenidos al tercer y cuarto panel. Juntamos los dos paneles, el de protección de datos y el de intermediarios de Internet. En el panel de protección de datos lo que queremos explorar es: tenemos visto cómo estos temas se ven penalmente, quizá con unos casos en el primer panel que fueron civiles y penales, y después la respuesta de la justicia penal, y ahora vamos a analizarlos desde el punto de vista de protección de datos.

Tenemos a dos funcionarios de la Defensoría de la Ciudad Autónoma de Buenos Aires, que está a cargo de la Ley de Protección de Datos de la Ciudad de Buenos Aires, que es la Ley N.º 1.845. María Julia Giorgelli y Eduardo Peduto nos van a comentar su visión de la Ley de Protección de Datos de la Ciudad de Buenos Aires. A nivel nacional, el Dr. Eduardo Cimato, de la Dirección Nacional de Protección de Datos Personales, estaba invitado y confirmado pero repentinamente no pudo venir porque tuvo un pequeño problema hoy: sus padres fueron víctimas de —nada grave— un

secuestro virtual, o sea que no fueron secuestrados sino que les sacaron información personal. El expositor tuvo que ir para estar sus los padres para ver que no pase nada, con lo cual, hablando de delitos informáticos, no pudo venir porque sus padres fueron víctimas de un delito virtual.

Después de ver la respuesta, cómo trata el derecho de protección de datos personales a la imagen y qué respuesta hay, tanto a nivel de la Ciudad de Buenos Aires como a nivel nacional se sumó Oscar Raúl Puccinelli, que es profesor de Derecho Constitucional en Rosario y juez de la Cámara de Apelaciones en Rosario, de local, y nos va a hablar. Tiene escritos ya tres o cuatro libros de protección de datos. Bueno, escribió un primer libro en Colombia, allá en el año 1999, cuando empezaba todo, de muy joven, después sacó una ley comentada de Astrea, y tiene artículos publicados en cualquier país del mundo sobre protección de datos, así que conoce mucho de protección de datos y nos va a hablar a nivel nacional y sobre todo internacional de cómo se aplica la Ley de Protección de Datos.

Y después tenemos la respuesta de los intermediarios —los llamamos así—, que sería qué papel juegan los intermediarios en todos estos temas, cómo pueden ayudar a prevenir o evitar que ocurran esta difusión no consentida de imágenes. Santiago Gini y Silvana Rivero nos van a hablar un poco del rol de los intermediarios, me imagino que hablarán de Belén Rodríguez y otros casos. Santiago Gini trabaja en OLX, es el gerente de Legales para toda América Latina de OLX. Silvana Rivero es ex alumna de San Andrés y ha dado clases con nosotros. En el CETyS también es investigadora junto con varios más que están acá presentes. Adelante y gracias.

María Julia Giorgelli: Muchas gracias por la invitación. En efecto, desde el Centro de Protección de Datos Personales de la Defensoría del Pueblo de la Ciudad, el derecho a la imagen lo trabajamos en el marco de la Ley Local de Hábeas Data N.º 1.845, y también por supuesto hacemos aplicación del artículo 53 del Código Civil.

Básicamente, trabajamos cuestiones que tienen que ver con los derechos de rectificación, su presión o autorización. Por nuestra competencia, no trabajamos aspectos relacionados con resarcimientos de daños y perjuicios, es decir, siempre lo hacemos dentro del marco de lo que es la

protección de datos personales, la privacidad y la intimidad. Trajimos acá algunos casos tramitados que dejamos abiertos al debate.

En primer lugar, podemos ver un caso que ya tiene sus años, es de 2013, y fue abierto de oficio. Una aclaración: la Defensoría emite recomendaciones que no tienen fuerza vinculante pero de algún modo van sentando precedentes, exponen posturas y analizan el derecho, sientan una postura. Además, muchas veces hacemos difusión de los casos apoyándonos en medios de comunicación con el fin de que los temas se debatan y tenga visibilidad. Volviendo, este es un caso que tuvo bastante repercusión, se conoció como "Chicas Bondi", su principal lema fue "Sin pose y sin permiso", o sea, una persona anónima, es decir que no se sabía muy bien quién era, tomaba fotos de mujeres en los colectivos y las subía a un blog. Después de eso también existió en un momento una especie de muestra de supuesto arte sobre la avenida Santa Fe, y el tema tuvo bastante repercusión en el ámbito de la ciudad. De manera que en esa oportunidad emitimos una recomendación haciendo hincapié en lo que tenía que ver con que las imágenes de estas mujeres habían sido captadas sin autorización de sus titulares, y además eran siempre mujeres que respondían a los patrones dominantes de belleza y que se las exponía como "cosas". Por ello sumamos una argumentación en relación a lo que se entiende por violencia simbólica y lo que garantiza la Convención de Belém do Pará. Y entre las recomendaciones se indicó la supresión del blog, y en ese momento el sitio se dio de baja por voluntad de su creador, y además de eso, pedimos la intervención de la CNRT [Comisión Nacional de Regulación del Transporte] y del Ente Único Regulador de Servicios Públicos de la Ciudad con el fin de que pongan un cartel informando sobre el tema y explicando que aún en el espacio público las personas tienen derecho a solicitar que terceros pidan la autorización para capturar y difundir sus imágenes.

Otro de los casos, uno típico de porno-venganza. Llegó por una denuncia de una empleada de un hospital público de la ciudad y desde el centro, en base a eso, consideramos nuestra competencia. Sobre este punto, aclaro: en el otro caso tomamos intervención porque eran situaciones que se daban dentro del espacio público del ámbito de la Ciudad de Buenos Aires.

Volviendo al de porno-venganza, la denunciante —una joven— refirió que su pareja había subido fotos íntimas al sitio Poringa.net y también a un grupo de Facebook del hospital en el que trabajaba, lo que invadió sin duda su intimidad y le generó una cantidad de problemas, al punto que se tuvo que cambiar de lugar de trabajo. La solicitud de baja, es decir de supresión, ante Poringa fue exitosa. Se solicitó la baja y ahí hay una nota. En ese momento la empresa tenía domicilio ubicable. Enviamos una comunicación formal y accedieron al pedido. En oportunidades, por una cuestión de legalidad, en el marco de las actuaciones administrativas que llevamos, necesitamos darles cierta formalidad a los pedidos. Hay veces que no nos es suficiente con la denuncia vía la plataforma virtual. O en algunas oportunidades denunciar o reportar algún contenido, un poco porque muchas veces los vecinos también necesitan tener alguna constancia y además porque a nosotros nos interesa seguir un camino de cierto control de calidad de cómo es efectivamente el procedimiento. En resumen, en esa oportunidad hicimos uso del artículo 3 de la Ley N.º 1.845, pedimos la supresión de esa imagen.

Siguiendo con el tema central del seminario, tenemos otros casos, que suelen ser denuncias realizadas por mujeres donde el Gobierno de la Ciudad no respeta la imagen en el espacio público, es decir toma imágenes para difundir algún servicio, en este caso el sistema público de bicicletas. La denunciante señaló que accidentalmente se vio en el Facebook del Gobierno de la Ciudad de Buenos Aires, advirtió que usuarios la calificaban, veinte "Me gusta", quince "Me gusta", algún comentario ("Estás un poco despeinada"), cuestiones que la sorprendieron y perturbaron dado que en ningún momento el Gobierno de la Ciudad de Buenos Aires le había pedido autorización de ningún tipo, ni formal ni informalmente, o de luego que fue publicada su imagen; simplemente de pronto se vio en esa red social. En ese contexto fue que contactó a la Defensoría. Casos así tenemos bastantes.

Uno de los primeros reclamos fue en el año 2013. Fue tomada la imagen de una chica mientras estaba en una plaza pública de la ciudad, era la plaza de la avenida Las Heras, y sin ella saberlo se ilustró la página web del Gobierno de la Ciudad que tenía que ver con temas de violencia de género. En este caso también, la titular del dato personal solicitaba

la supresión, es decir, que se diera de baja su imagen. En resumen, en ningún caso las personas prestaron acuerdo para ser retratadas y luego difundir su imagen, y en general la difusión es siempre en la web.

En relación con estos casos, desde la Defensoría tenemos la postura de que aun en el espacio público es necesario solicitar autorización al titular del dato —después podríamos discutir si la autorización es tácita o expresa—, que allí las personas tienen una expectativa de anonimato, creen que pueden circular sin ser identificados en pos de la protección de su privacidad.

Entonces, salvo que exista una ley como, por ejemplo, ocurre con la de seguridad en la ciudad, que contempla aspectos de videovigilancia y por medio de la cual se "autoriza" a captar la imagen de las personas en el espacio público, siempre es necesario que cada persona autorice a quien va a capturar o difundir la imagen.

En esta línea, y para ir cerrando, trajimos casos relacionados con imágenes en el espacio público o situaciones que debimos analizarlas con perspectiva de género. Hay acá alguna mezcla. Tres de ellos revelan un tratamiento peyorativo respecto de los derechos de las mujeres. En algunos casos nosotros los derivamos, en otros realizamos gestiones administrativas. En algunos de ellos solicitamos reuniones a las cámaras de medios comunicación, como por ejemplo ADEPA [*Asociación de Entidades Periodísticas Argentinas*] o Fopea [Foro de Periodismo Argentino]. Hacemos ello porque, al ser difundidos por la web, hay ahí un supuesto vacío respecto de quién debe tratar esos casos y, aclaro, nosotros no estamos de acuerdo con que todo deba judicializarse, dado que ello resulta muy difícil para la media de las personas. Volviendo, por ejemplo, el caso N.º 21.050 y el N.º 17.790 son casos que muestran situaciones de una mujer víctima de una violación en el año 96 y que todavía hoy aparece en uno de los principales buscadores, y además en el primer lugar, ello con sólo consignar su nombre en el buscador. En estos casos, desde la Defensoría no creemos que haya conflicto con el derecho a la libertad de expresión, y consideramos que el caso debe ser abordado desde la perspectiva de los datos personales. Concretamente, la denunciante manifestó que denunció al violador en la justicia en su momento, que hoy ya está libre, que ella tiene hijos y una vida, entonces se observa allí una cantidad de datos

personales e información privada, y además datos que se convierten en sensibles, que de seguir circulando además revictimiza a las mujeres.

En el otro caso, el medio de comunicación focaliza su nota en la esposa, que es la persona conocida, cuando es él quien generó la violación, es decir, como ella era hija de desaparecidos, la noticia circula todo el tiempo con eso y hoy es posible detectar su información personal y relativa a su intimidad en un buscador solo consignando el nombre de ella. Desde la Defensoría no estamos de acuerdo con ese acceso indiscriminado, permanente y atemporal a información personal.

Un caso similar respecto de estas características es el blog "Patentes y Travestis" también, donde hay una mirada prejuiciosa respecto de este colectivo. Las fotos son del Parque 3 de Febrero, gerenciado por el Gobierno de la Ciudad, y por eso la Defensoría tomó intervención en el caso. Tomamos contacto con el buscador, quien argumenta aspectos de libertad de expresión, y con el GCBA. Lamentablemente nuestras acciones fracasaron, dado que el blog sigue activo; hace años que están las mismas fotos, que muestran caras identificables y patentes de auto, por ejemplo.

Y con relación al derecho a la imagen, tomamos intervención en varios casos sobre el uso de imagen de niña y niños en las escuelas. En general, el Gobierno de la Ciudad hace circular una autorización pero que tiene vicios. Es general, muy vaga, genérica, que permitiría hacer uso de las imágenes de los chicos bajo cualquier circunstancia, contexto, no se sabe muy bien si su tratamiento será con fines educativos, o sea, no hay ningún dato concreto y específico en esos formularios de autorización de uso de imagen, para qué se va a usar la imagen concretamente. Algunos de estos casos fueron abiertos de oficio, y el resto han sido denunciados por padres, muchos de nenas.

Muchas gracias.

Eduardo Peduto: Tomo yo desde otra punta. Lo que decía María Julia [Giorgelli], yo quisiera hacer énfasis fundamentalmente en el caso N.º 17.790, porque el caso al que se refería María Julia, esta chica fue violada cuando era menor de edad. Y el juez que en su momento llevaba la causa consultó a la madre y a ella porque había presión de varios medios que querían acceder al caso. El juez criteriosamente les solicitó auto-

rización, ellos se la negaron, y no obstante algunos medios consiguieron los datos por otro lado, publicaron el caso de esta chica, tanto ella como la madre en representación de ella hicieron una acción civil contra el medio, en este caso es *Clarín*. Concretamente, ganaron la causa civil en primera instancia ratificada por la cámara. Lo único que la cámara bajó fue el monto de la indemnización, pero lo preocupante de esto es que sigue estando en la edición digital de *Clarín* un caso del año 96, y se lo hemos pedido por todos los medios, y dicen que tienen "dificultades técnicas".

Acá hay dos cuestiones que me gustaría señalar. A algunas se refirió María Julia. Con el Gobierno de la Ciudad debemos haber peleado durante, fácil ocho años, para que hicieran carne de que la imagen es un dato personal. La propia Procuración de la Ciudad tenía dictámenes negando que la imagen era un dato personal. Recién los últimos tiempos han aceptado que la imagen es un dato personal.

Y la otra cuestión a la que hizo referencia María Julia en cuanto a nuestras limitaciones, desde la 1.845, que apela solo a los bancos públicos de datos, nosotros hemos intentado darle una vuelta de tuerca a esto con una cuestión, porque hay un vacío legal no solo de la ciudad sino a nivel nacional, es lo que se refiere justamente a todo lo que tenga que ver con Internet, es decir, las leyes. La de la ciudad es lógico, porque solo se refiere a los bancos públicos, pero la nacional tiene un gran hueco en ese momento, y el proyecto que está en danzas… lamento que no haya venido el representante de la Dirección Nacional. El proyecto que está en danza es absolutamente confuso y ambiguo respecto al tema, por ejemplo, de la transferencia internacional de datos. Son temas que dejo ahí planteados porque me parecen importantes.

¿Cuál era la vuelta de tuerca que hemos intentado darle? Es la siguiente. Está bien, la ley 1.845, desde el punto de vista acotado, solo nos brinda la posibilidad de intervenir en el caso de bancos públicos de datos. Pero hete aquí que, como autoridad de aplicación de la Ley de Protección de Datos Personales está la Defensoría del Pueblo. Y la Defensoría del Pueblo, tanto por la Constitución de la Ciudad como por la Ley N.º 3, en realidad debe delegar por la protección y vigencia de los derechos humanos respecto de los habitantes o aquellos que circulen por la ciudad, con lo cual hemos intentado extenderlo y trascender la 1.845.

Y lo último para compartir con ustedes: estamos avanzando en un proyecto muy interesante, bajo jurisdicción de la Defensoría del Pueblo de la Ciudad. Se va a llevar un registro único de violencia de género. En este momento debe ser la quinta reunión que tenemos. Es un esquema muy interesante. Está interviniendo la Dirección de Estadísticas y Censo de la Ciudad, el Consejo de la Magistratura, la Dirección de la Mujer, la Policía de la Ciudad, está el Inadi [Instituto Nacional contra la Discriminación, Xenofobia y el Racismo], está la OAV [Oficina de Asistencia a la Víctima] de la Corte Suprema de Justicia de la Nación, y justamente uno de los vectores de este registro único de violencia tiene que ver justamente con el tema de Internet. Y acá digo, como reflexión final que quería compartir con ustedes, Internet en su momento generó muchas expectativas acerca de la apertura democrática, igualitaria, la accesibilidad que eso significaba para muchos ciudadanos y ciudadanas del mundo que eran ajenos al acceso a la información, pero progresivamente se ha transformado en otra estructura centralizada, donde la garantía de la igualdad de acceso a la información está bastante comprometida.

¿Y cuál era la reflexión que yo quería compartir con ustedes? El vértigo tecnológico hace que la primera reacción sea de asombro. La segunda es fascinación, de ahí pasamos al encandilamiento, y el encandilamiento permanente produce ceguera, y yo creo que ese es uno de los riesgos que corremos si no tenemos una mirada crítica, constructiva, aceptadora por supuesto de los grandes avances que significa la transformación tecnológica, pero de la manera tal que esa transformación tecnológica signifique un empoderamiento para la ciudadanía y no que la tecnología se apodere de la ciudadanía.

Eso es lo que quería compartir con ustedes.

Oscar Raúl Puccinelli: Buenas tardes. Muchas gracias a Pablo [Palazzi] y a los demás miembros del CETyS por la invitación a participar en este panel, que involucra un tema tan trascendente como extenso y en el que voy a ser lo más breve posible.

En el tema del *revenge porn* que estamos tratando tienen directa incidencia las reglas emergentes de la Ley de Protección de Datos Personales, puesto que las imágenes de contenido sexual diseminadas a fin de

perjudicar a una o más personas que se encuentran en ellas son datos de carácter personal que caen bajo la órbita de dicha norma.

Es que sin duda alguna se trata de imágenes que: a) están digitalizadas del mismo modo que un nombre o dirección (es decir, a través de unos y ceros); b) refieren al menos a una persona identificada o identificable (lo que las convierte en un dato personal); c) son tratadas en un sistema de información (Internet), que a través de una herramienta tecnológica (sus motores de búsqueda) toma información de diversas bases de datos a fin de conformar, a requerimiento del internauta, verdaderos bancos de datos personales; y d) refieren a actos íntimos de las personas, y por involucrar información sobre la vida sexual de estas se convierten en datos sensibles o, en la terminología de otras legislaciones, datos especialmente protegidos.

Es cierto que la Ley N.º 25.326 debe ser actualizada porque su matriz se corresponde a la era "pre-Internet", pese a que fue sancionada diecisiete años después de la adopción del protocolo TCP/IP (esto porque su fuente directa es española, concretamente la Ley Orgánica sobre el Régimen d e Tratamiento Automatizado de Datos de Carácter Personal, de 1992, que se dictó en respuesta a los requerimientos emergentes del Convenio Europeo de 1981, esto es, tiempos de la primitiva Arpanet), pero también lo es que alcanza mínimamente con los derechos y principios reconocidos en ella para enmarcar el tratamiento de este tipo de información y establecer la ilegalidad de su cesión a terceros sin el consentimiento explícito de los titulares de los datos cuyas imágenes han sido captadas y están siendo o pretenden ser difundidas.

Merece a este respecto tener presente que ya en el artículo 1 de la ley, siguiendo la redacción de la Constitución Española de 1978 y la LORTAD[12] también española de 1992 (que fue *aggiornada* en 1999, es decir, un año antes de aprobada la Ley N.º 25.326, novedad que el legislador local parece no haber conocido) se declara como objetivo preeminente el de "garantizar el derecho al honor y a la intimidad de las personas", y aquí precisamente se está ante un dato de naturaleza íntima, más concretamente "sensible" en los términos de la ley según la definición que del mismo se hace en el artículo 2 (dato "referente a la vida sexual") y que

[12] Ley Orgánica de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal.

en el artículo 7 quedan sujetos a un régimen especial, de tutela reforzada ya que nadie puede ser obligado a proporcionarlos y solo pueden ser tratados por razones de interés general o cuando estén disociados (salvo que contaran, conforme lo disponen los artículos 5 y 6, con consentimiento "libre, expreso e informado del titular de los datos", que en todo momento puede revocar para el caso de la cesión o transferencia de esos datos (artículo 11).

El cuadro tutelar se completa a poco que se comprenda que el tratamiento de datos no puede hacerse de manera contraria a las leyes o a la moral pública (artículo 3); que los tratados no deben ser excesivos en relación al ámbito y finalidad para los que se hubieren obtenido; su recolección no puede hacerse por medios desleales, fraudulentos o contrarios a la ley, ni utilizarse "para finalidades distintas o incompatibles con aquellas que motivaron su obtención", debiendo "ser destruidos cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubiesen sido recolectados" (artículo 4).

Además, el titular goza del derecho a la información sobre el tratamiento (artículo 6) y entre otros derechos "arco" a la confidencialidad de los datos sensibles que estén correctamente tratados (si es que solo se pretende limitar el consentimiento para el tratamiento a las personas que estuvieron involucradas en una actividad sexual y solo se pretende inhibir su exhibición a terceros) y a la supresión de los datos ilegalmente tratados (artículo 16), previéndose un esquema de control administrativo (artículos 29 a 31); legal, a través de sanciones penales (artículo 32) y judicial, a través de la acción de hábeas data (artículo 33).

En estos casos suele ocurrir que la recolección del dato se haya realizado por medios lícitos y con el consentimiento expreso y explícito de las personas involucradas en determinada actividad de índole sexual, lo que implica la posibilidad de registrarlos pero no de realizar sin consentimiento las restantes operaciones de tratamiento (que conforme las define el artículo 2 consisten en las "operaciones y procedimientos sistemáticos, electrónicos o no, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción, y en general el procesamiento de datos personales, así como también su cesión a terceros a través de co-

municaciones, consultas, interconexiones o transferencias") y mucho menos utilizarlos para "finalidades distintas o incompatibles", como sería claramente la difusión hacia terceros o cualquier otra forma dañina de tratamiento de los datos.

Tal vez el tema más polémico se centra en la posibilidad de exigir la destrucción de los datos cuando existió una relación sentimental que culminó y en cuyo contexto se tomaron consentidamente las imágenes (tal el caso en que exigiésemos la supresión de las imágenes en el ordenador de una ex pareja que desea mantenerlos como parte de sus "papeles privados", sin transferirlos a terceros). Esto porque, si bien al abrigo del artículo 4, apartado 7, los datos "deben ser destruidos cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubiesen sido recolectados", el artículo 16, apartado 5 dispone que la supresión "no procede cuando pudiese causar perjuicios a derechos o intereses legítimos de terceros", y podría entenderse en ese perjuicio que el interés legítimo de un tercero estaría dado por la exigencia de borrar un archivo que no ha sido utilizado contra la ley (ni se pretende utilizar en dicho sentido) y que responde a un hecho personal que desea mantener para su recuerdo.

La cuestión se pone todavía más polémica a poco de que se advierta que en las normas más actualizadas, como en el Reglamento General de Protección de Datos de la Unión Europea, atendiendo a las sustanciales modificaciones en el tratamiento de los datos personales que no fueron tenidas en las normas previas que respondían a un contexto de Internet 1.0, esto es, sin redes sociales (donde ahora existe un gran predominio de inclusión de imágenes que involucran a terceros), se están flexibilizando las pautas del consentimiento, e incluso en las directrices relativas al derecho a la portabilidad de los datos emitidas por el Grupo de Trabajo del Artículo 29, se flexibiliza el concepto de "dato relativo al interesado" porque el derecho de portabilidad tiene como objeto poder transferir todos los datos que alguien tenga en una plataforma (datos de terceros incluidos) tanto para sí como para otro proveedor de servicios de la sociedad de la información, sin intervención de terceros. Esto, más allá de que el proveedor que actuará como receptor de esos datos deba evaluar si los datos a transferir sean compatibles con las finalidades que tendrá el nuevo tratamiento.

El documento expresa a este respecto lo siguiente: "En muchas circunstancias los responsables del tratamiento procesarán información que contiene los datos personales de varios interesados. En ese caso los responsables del tratamiento no deberán tener una interpretación excesivamente restrictiva de las frases, datos personales que conciernen al interesado. A modo de ejemplo, registros telefónicos pueden incluir en el historial de cuenta del abonado datos de terceros participantes, llamadas entrantes y salientes, y aunque los registros van a contener por lo tanto datos de terceros o de multitud de personas, los abonados deben tener la posibilidad de que se les proporcionen dichos registros en respuesta a solicitud de portabilidad de los datos. Sin embargo, cuando en tales registros se permita a un nuevo responsable del tratamiento, dicho nuevo responsable del tratamiento no debe procesarlos para ningún fin que pueda afectar negativamente los derechos y libertades".

De todos modos, la flexibilización que caracteriza a las normas más actuales también lleva a considerar nuevas herramientas (que obviamente no están contenidas desde lo expreso en la ley argentina de protección de datos, por su vetustez), como el derecho al olvido, brevemente mencionado en el artículo 13 del Reglamento Europeo de Protección de Datos y que ha sido excluido en algunos proyectos de reforma a leyes latinoamericanas (el de reforma a la ley 25.326 lo excluye) o bien fue colocado de manera subrepticia en nuevas normas y proyectos de ley en los cuales se pretenden actualizar las leyes de protección de datos (la ley mexicana de protección de datos personales en posesión de sujetos obligados, de 2017, lo incluye sin mencionarlo al reconocer el derecho a la oposición al tratamiento cuando si bien este pueda considerarse lícito, puede causar daños desproporcionados al titular o a terceros).

Rebobinando un poco lo expuesto, el tratamiento de imágenes de contenido sexual es privado y encuentra diversas herramientas —que en la práctica no resultan ser todavía de lo más eficaces— para enfrentar un caso de *revenge porn*, que exige de procedimientos ágiles, mente abierta y gran sensibilidad por parte del Estado, porque de lo contrario estaremos favoreciendo linchamientos digitales a manos de personas desaprensivas y contribuyendo al engrosamiento de las filas de los denominados *walking virtually dead*.

Desde el punto de vista judicial, además de lo que pueda hacerse desde el ángulo penal (tema que ya fue analizado en los paneles anteriores), además del hábeas data, debe poder acudirse a otras herramientas procesales que son reclamadas por la legislación de fondo, como las medidas de tutela preventiva en sus diversas formas, medidas autosatisfactivas, etcétera.

En este punto bien vale recordar lo dispuesto por el Código Civil y Comercial en cuanto al deber de toda persona de prevenir daños —en concreto de: a) evitar causar un daño no justificado; b) adoptar, de buena fe y conforme a las circunstancias, las medidas razonables para evitar que se produzca un daño, o disminuir su magnitud; y c) no agravar el daño, si ya se produjo— (artículo 1.710) y en lo relativo a la "acción preventiva", que "procede cuando una acción u omisión antijurídica hace previsible la producción de un daño, su continuación o agravamiento", concurra o no algún factor de atribución (artículo 1.711).

La judicatura, muchas veces al calor del clamor de la doctrina, ha dado ejemplos reiterados de soluciones innovadoras cuando las reglas imperantes respecto de las nuevas tecnologías de la información y de la comunicación generaban respuestas inadecuadas a problemas acuciantes que no podían ser resueltos por la vía de las reglas imperantes. En este punto, el célebre opúsculo de Warren y Brandeis publicado en 1890 en *Harvard Law Review* titulado "The Right to Privacy"[13] provocó una serie de importantes reacciones judiciales frente a publicaciones de la prensa lesivas del derecho a la intimidad o al honor.

Así, por ejemplo, en el célebre caso "Melvin v. Reid", fallado en 1931 por la Corte de Apelaciones de California, se condenó al productor de la película *The Red Kimono* por haber recreado en el film la vida de una trabajadora sexual, con su verdadero nombre, lo que permitió que todo su nuevo entorno se enterase acerca de un pasado lejano que quería dejar atrás. Resultados similares se produjeron inmediatamente, verbigracia, en el caso "Mau v. Rio Grande Oil", resuelto en 1939 por una corte de distrito de California, donde se entendió violatoria de la privacidad la recreación por radio de un asalto que había sufrido una persona, identificándola, y en otros antecedentes importantes del siglo pasado, especialmente en Estados

[13] Samuel Warren and Louis Brandeis, "The Right to Privacy", *Harvard Law Review*, 4, 193 (Dec. 15, 1890).

Unidos, Alemania y en Francia, donde se aplicó el criterio protector de la privacidad frente a informaciones verdaderas que en principio podían ser lícitamente publicadas, pero cuya divulgación producía un daño injustificado a sus protagonistas, por ejemplo relacionadas con condenas penales cumplidas (caso del crimen de los soldados de Lebach, del Tribunal Constitucional Alemán, de 1973) o imágenes de una película donde se representaba, muy ligera de ropas, a una amante de un conocido asesino serial[14] e incluso referidos a antiguas deudas, saldadas o no[15].

La protección de la intimidad incluso se ha extendido a actos voluntariamente realizados frente al público general, donde la persona voluntariamente renunció a su derecho a la privacidad, por ejemplo al exponerse desnuda en el medio de una protesta. La jurisprudencia francesa falló a favor de la mujer que había iniciado una demanda contra la empresa periodística que difundió su imagen sin recurrir a mecanismos de difuminación, avalando el reclamo de la mujer en cuanto solo había aceptado desnudarse frente a los manifestantes y no ante toda Francia.

La evolución de la jurisprudencia gala diferenció entre personas con y sin notoriedad pública, y atendiendo a la posibilidad del consentimiento implícito para su difusión, que no se presume de manera general aun cuando se esté frente a *vedettes* que por su trabajo se hayan expuesto previamente a la curiosidad y a la notoriedad pública, o incluso frente a trabajadoras sexuales cuyas fotografías fueron captadas en la calle donde desenvolvían los preliminares del propio trabajo. Incluso en 2004 el Tribunal Europeo falló a favor de la princesa Carolina de Mónaco por la publicación de una serie de fotografías "que afectaban al respeto de su vida privada", recordando la importancia fundamental que reviste la protección de la vida privada para la expansión de la personalidad de cada uno, protección que va más allá del círculo familiar íntimo y afirmando que cualquier persona, incluso conocida de la opinión pública, debe poder beneficiarse con una esperanza legítima de protección y respeto de su vida privada, y en consecuencia debe respetarse su imagen.

[14] Caso "Landrú", resuelto por la Corte de Apelaciones de París, 1967.

[15] Sentencia T-414 de la Corte Constitucional de Colombia, de 1992, y ya en este siglo, caso "Costeja v. Google", resuelto por el Superior Tribunal de Justicia de la Unión Europea.

Por último, en función del tiempo asignado para mi intervención, quiero llamar la atención acerca de los caos en los que se recurre a técnicas de anonimización de los datos, como puede ser la difuminación de las imágenes (hipótesis donde los datos personales dejan de serlo y ya no están alcanzadas por la ley de protección de datos). Si bien una difuminación puede parecer suficiente mecanismo de anonimización, a veces no lo es porque, por ejemplo, alguien puede difuminar en su cuenta de Facebook una imagen de la cara de quien está fotografiado a su lado, pero del contexto del resto de los datos a los que se puede acceder es factible determinar de quién se trata. Incluso a veces es necesario ampliar la difuminación a otras partes específicas del cuerpo y no solamente a la cara, por ejemplo si alguien tiene tatuajes, porque de acuerdo a la imagen que esté tatuada y su ubicación en el cuerpo puede ocurrir que esa persona no identificada sea identificable.

Finalizo agradeciendo nuevamente la invitación que me cursaron y felicito a los organizadores por el éxito de un evento que ha puesto su foco en un tema de tanta actualidad y trascendencia como la protección de las imágenes en el mundo digital.

Santiago Gini: Gracias. No sé si les pasa, pero cuando tienen que preparar algo, un examen, una charla, empiezan a ver muchas cosas de su vida cotidiana con los "anteojos" de eso que están preparando. Justo esta semana me pasó que Fernanda, la coordinadora del CETyS, me pidió mi currículum, y como trabajo hace cuatro años en el mismo lugar, tuve que buscarlo. Y ahí veo que hace nueve años publiqué un artículo que se llamaba muy parecido a esta charla, "Intermediarios de Internet y libertad de expresión". Y esta charla se llama "El rol de los intermediarios y el problema de la libertad de expresión en Internet". Dos primeras conclusiones: la primera es qué poco evolucioné, ya que hace nueve años que hago lo mismo. Y la segunda es el matiz.

Yo no sé si plantearía como el problema de la libertad de expresión. Yo digo: la libertad de expresión siempre tuvo un costo. Y en realidad no es la libertad de expresión el costo. El costo deriva del libertinaje o de las acciones que no están enmarcadas propiamente en lo que es el contenido, el núcleo de la libertad de expresión. Y eso pasó históricamente y te-

nemos un montón de jurisprudencia pre-Internet, y ahora nos pasa que, penetrando Internet en nuestra vida cotidiana desde que nos levantamos hasta que nos vamos a dormir, empiezan a aparecer estas causas.

Yo creo que ya a esta altura podemos decir que hablar de la nube o del mundo virtual son metáforas que nos pueden servir en algún sentido, pero la libertad de expresión es en el mundo real, por más que se materialice en un *tweet*, se está materializando en el mundo real y el daño se materializa en el mundo real, no queda en el mundo virtual.

Superando eso filosófico trato de ir a algo un poco más concreto, y cuestiones que creo que no se dijeron a lo largo del día y por eso va a quedar un poco más inorgánico lo que quiero plantear.

El otro acento de la charla no está en el problema sino en el rol de los intermediarios. Creo que el rol de los intermediarios es un rol activo en la tutela de la neutralidad como principio de no discriminación. No es el intermediario el único actor, y después me gustaría charlar un poco sobre el Estado; sobre los ciudadanos algo se dijo, sobre el resto de los actores. La tutela de la neutralidad como principio de no discriminación nos va a permitir no poner en riesgo muchísimos derechos, entre otros la libertad de expresión, entre otros el debido proceso, entre otros el desarrollo del trabajo, y así todo el resto de los derechos fundamentales.

Creo que habiendo pasado nueve años no contando con una ley, a pesar de que haya habido distintos proyectos, habla un poco también de nuestra poca exigencia hacia un Estado que ya con quince años de Internet hipermasiva no puede resolver un problema básico. Hay países en Europa que tienen normas desde 2001, y antes también tenían en el 95. Un Estado que no educa, o educa mal o poco. Un Estado que poco castiga, un Estado que poco investiga. ¿Y por qué hablo, hago énfasis en el Estado? Más allá de que es siempre lo más fácil, porque creo profundamente que es verdad, creo que muchas veces se les quieren implicar responsabilidades a los intermediarios por las falencias del Poder Judicial. En el primer panel hablaban de "Yo lucho contra dos cosas", y una era el Poder Judicial.

Creo que el problema excede al Poder Judicial, y no es solamente el Poder Judicial. Pero, bueno, es uno de los partícipes necesarios para que cualquier causa termine. No sé, si necesitás ocho años para pasar a pri-

mera instancia… Esta semana me salió una caducidad de una causa que llevo desde 2008 y que todavía no había llegado a alegatos.

En los ciudadanos un poco también, y lo decía el doctor Azzolin, ciudadanos que a veces no nos oponemos a lo que es la lesión de derechos, que a veces no nos importan que un intermediario haga tal o cual cosa, y que sea justo o menos justo, o que sea ético o menos ético.

Y ahora hablo de los intermediarios, y cuando hablo de los intermediarios lógicamente uno tiende a pensar en esas compañías que valen más de trescientos billones de dólares, quiere decir que son muchísimas veces más grandes que las compañías más grandes de Argentina juntas, pero los intermediarios son todos, son Google, son Facebook, pero también es un pequeño blog, es un pequeño diario, es cualquier página profesional que se abra a comentarios. Y también ahí caen intermediarios de su posición y de sus medios, puede tener posturas más éticas o más profesionalmente amigables con una sociedad más justa.

Y así como se opta, por ejemplo, por alimentos en los que se prueba que no se ha lastimado a tal grupo, que no se ha hecho de tal forma, por ahí los ciudadanos deberíamos, hoy en 2017, empezar a plantearnos qué tipos de empresas queremos que sean nuestros intermediarios, y dejar de desentendernos. [Edward] Snowden fue bastante ilustrativo, y sin embargo creo que el ciudadano promedio sigue viviendo una ilusión.

Vuelvo al artículo de hace nueve años: ¿qué pasó? La verdad es que pasó mucho y pasó poco. Tenemos fallos de la corte, lo cuales han sido bastante iluminadores o bastante pacificadores en el sentido de que ya no tenemos, primero, cuatro años para pelearnos a ver si tenemos que ir a federal o a civil, por más que sigan pasando esas cosas. Tenemos algunas pautas que sabemos que cualquier juez que no quiera que su sentencia termine siendo no aplicada, tiene que respetar. Creo que quedó atrás toda la postura de responsabilidad objetiva, la visión del intermediario como editor.

Algo que me causa gracia es que nos encanta hablar de las nuevas tecnologías y sin embargo, en cuanto podemos, queremos usar los títulos viejos. “Ah, esto es como Telefónica.” No, no es como Telefónica. Es Internet, o sea, hay una parte de Telefónica como proveedor de servicios de Internet y ahí puede servir, pero el complejo es distinto.

Entonces creo que el mundo desarrollado no oscila entre una inmunidad absoluta y una condicionada, sino entre distintos tipos de inmunidades condicionadas para los intermediarios. Siempre está el riesgo de imponer obligaciones difusas. Creo que, en ese sentido, por ahí uno de los considerandos del fallo de María Belén Rodríguez no es tan feliz en ese sentido. Qué son lesiones contumeliosas evidentes.

Ahora quiero distinguir muy claramente lo que es un deber legal de lo que dije antes, de lo que es un compromiso ético. Si en mi compañía no quiero, no sé, en OLX no aceptamos temas de pornografía. Saquémosle la palabra "ética", es de política corporativa. Lo que no quiere decir que el Estado pueda prohibir la venta de pornografía. Ahora en esta compañía optamos por esto, no somos los únicos.

Creo que dentro de ese marco regulatorio que cada vez queda más definido dentro de inmunidad condicionada, sería un error regular para Google y Facebook. Hay que regular para todos los actores de Internet. De hecho, una de las cosas que más me gustan de Internet y por las cuales, para decirlo coloquialmente, me metí de lleno hace varios años, es su capacidad democratizadora, su capacidad de que cualquiera con el talento y la suerte suficiente puede ser la próxima multinacional y ya no necesita de licencias, no necesita ser "hijo de", no necesita estar en el grupo de medios tal. Hoy el talento puede hacer que tengas una vidriera global por un muy bajo costo.

Creo que tengo algunas diferencias con los fallos de la corte, algunas particularidades. Me meto un poco en lo que se hablaba hoy de la Ley N.º 11.723. Vengo un poco de la rama de la propiedad intelectual, porque el Derecho de Internet es algo raro, no hay una norma de Internet. Hay un montón de normas que tienen efectos sobre Internet. Y cuando opté por meterme en este ecosistema jurídico, o esta rama del Derecho difusa, opté por el lado de propiedad intelectual. Y en ese sentido por ahí, un poco lo que se decía recién del fallo de Francia, acá la Ley N.º 11.723, que te habilita expresamente a que si vos estás en un acto, una manifestación pública, un acto de interés público, si esa imagen es recogida por un medio en el contexto de dar a difundir esa noticia, no habría que darle autorización ni pagar regalías ni nada.

Con respecto a la estrategia de Tommy Lee con aquel video con Pamela Anderson de monetizarla de alguna forma como una obra, por ahí una de las diferencias entre el *copyright* y el derecho de autor es notable porque el *copyright* hace acento en la copia y el derecho de autor pone el acento en el autor, y yo digo, más allá de lo que dijo el doctor Azzolin, que creo que es verdad, que no hay que naturalizar los institutos, es una jugada peligrosa. Entonces decís: ¿de quién es la obra? Porque por ahí era de dos partícipes o más, ¿y qué hacemos? Porque no me pagaste por esta obra, ni la registraste, o deberías registrarla para poder reclamar.

Yo creo que las soluciones del Estado deben ser más sensatas y tomar la problemática desde su propia problemática, y no agarrar un instituto que existe. De vuelta, agarrar lo de siempre y lo que usábamos para perseguir un tipo que vende DVD en la calle o una fábrica de DVD, como fue en su momento, no sé si se acuerdan del nombre de un periodista y sus esclavos camboyanos. Facturaba más que muchísimas pymes de Argentina y repartía DVD por toda Argentina.

Creo que estamos en una etapa de transición, así es como hoy se ven distintos debates. Cierro con estas dos ideas. Estamos en el debate de qué rol, se habla de los OTT y "*level the playing field*".

Creo que estamos en un proceso, y encasillar un proceso es riesgoso. Finalmente, creo que vale la pena seguir profundizando en las medidas tecnológicas, ya sea tanto desde el Estado de manera preventiva o para facilitar la punición, como de las empresas para disminuir los riesgos de lesiones. Un poco con todo lo que pasó en Estados Unidos, Facebook entre otras empresas, pero recuerdo muy patentemente la de Facebook, en Estados Unidos, que solicitaba en el diario diciendo: "En virtud de lo sucedido, esto es lo que vamos a hacer, y vamos a contratar más gente, vamos a poner un sistema de inteligencia artificial para medir esto, vamos a…". Entonces, para mí eso es un compromiso de una compañía multinacional positivo. Ahora, ¿yo le puedo exigir eso a un blog que podamos hacer nosotros? De hecho, en el CETyS tenemos un blog y no podríamos afrontar ese costo. Lo que quiero decir es que el Estado no me debería imponer un costo de editor y de inteligencia artificial, y tener una maratón de abogados analizando si el *hashtag* de la Dra. Pignata

#Boudouchorizo es ilegítimo o no porque es una figura pública pero claramente están injuriando porque todavía no hay una condena. Bueno, eso no se le podría decir. Así que bueno, creo que dije un poco todas las ideas que quería decir y dejamos a las preguntas.

4. Cierre y conclusiones de la jornada

Pablo Palazzi: Gracias a todos y todas por participar esta tarde en el seminario. Hemos podido ver cómo, cada vez con más frecuencia, estos hechos relacionados con la violencia de género digital se encuentran con numerosos problemas en el mundo jurídico.

El primero es la falta de clara recepción legislativa en el Código Penal o en otras normas, lo que dificulta el encuadre de la investigación en esta clase de casos. Los casos en la realidad son así, complejos y variopintos: van desde un simple hostigamiento aislado hasta acosos constantes y extensos a lo largo de años en redes sociales e Internet. Desde simples insultos hasta publicación y viralización de videos y audios de naturaleza sexual, a veces con la inclusión de link al perfil verdadero de la víctima en una red social, incluyendo su teléfono laboral o personal, o el envío de dicho contenido a sus allegados virtuales, compañeros de colegio o colegas laborales.

Se termina aplicando una figura contravencional genérica (porque es lo único que hay en la Ciudad de Buenos Aires), hasta amenazas, coacciones, chantaje o extorsión, además de difusión indebida de correspondencia privada y a veces acceso no autorizado a sistemas informáticos o incluso las normas penales sobre protección de datos personales. Todas estas figuras tienen un denominador común: la violencia de género en ambientes digitales, a veces amparadas, como se dijo ya, en el anonimato de Internet. Lo que lleva a plantearnos si no se debería pensar en un agravante en algunos de estos supuestos.

El segundo problema es la dificultad que presentan los operadores judiciales para enfocar estos casos, y obtener la prueba de cargo necesaria para llevar adelante el caso. La prueba de subida del video, o de la dirección IP está en servidores en el extranjero, o en servidores anonimizados, o con

un ISP[16] que se niega a colaborar a menos que le llegue un exhorto que demora meses (a veces años).

En tercer lugar, falta poner énfasis en la educación de estos temas a todos los niveles, no solo en la escuela y en la universidad sino en trabajos, la academia y las autoridades públicas que deberían encarar el tema seriamente como una política central para que la Convención de Belem do Pará esté plenamente vigente en ambientes digitales.

Todos estos problemas quedaron expuestos hoy en las exposiciones de los operadores legales y judiciales del seminario así como de los abogados que expusieron casos que llevaron en tribunales y hasta de las propias víctimas que contaron casos concretos y nos demostraron lo que implica sufrir la violencia digital.

Les agradecemos a los expositores por su participación y esperamos que las experiencias y conclusiones vertidas en este seminario sirvan para mejorar la legislación pendiente en el Congreso Nacional sobre la materia.

[16] Proveedor de servicios de Internet (en inglés, *Internet Service Provider*).

Jurisprudencia

JURISPRUDENCIA ARGENTINA

Caso Uber - Alcance de medida cautelar

El TSJ de la Ciudad de Buenos Aires revocó una sentencia por la que se ordenaba la clausura y bloqueo de la página web y aplicaciones de UBER.

COMPETENCIA EN RAZÓN DEL TERRITORIO. Cámara de Apelaciones en lo Penal, Contravencional y de Faltas ordena la clausura/bloqueo de la página web, plataformas digitales y aplicaciones de compañía dedicada al transporte de pasajeros —"Uber"— en todo el territorio del país. RECURSO DE QUEJA: procedencia. ORGANIZACIÓN JUDICIAL. Régimen federal. Límites de la Ciudad de Buenos Aires. CONSTITUCIÓN DE LA CIUDAD AUTÓNOMA DE BUENOS AIRES. Art. 8. Magistrados que en la resolución adoptada exceden el ámbito de su jurisdicción. LEYES 26.032 y 27.078. LIBERTAD DE ACCESO A LA INFORMACIÓN A TRAVÉS DE LAS REDES QUE SE VULNERA. Se revoca la resolución recurrida.

"NN (UBER) s/ queja por recurso de inconstitucionalidad denegado en: 'Incidente de apelación por clausura/bloqueo de página web en todo el país en autos: NN (UBER) y otros s/ infr. art(s). 83, 73 y 74 CC" - TRIBUNAL SUPERIOR DE JUSTICIA DE LA CIUDAD DE BUENOS AIRES - 18/06/2018 Expte. nº 14483/17 "NN (UBER)"

Buenos Aires,18 de junio de 2018.

Vistos: los autos indicados en el epígrafe.

1. Los abogados defensores de Mariano Otero dedujeron queja (fs. 64/94) por denegación del recurso de inconstitucionalidad cuya copia acompañaron a fs. 23/59. Allí cuestionaban la decisión de la Sala II que había confirmado la de primera instancia en cuanto hizo lugar a la solicitud del MPF de extender a todo el territorio nacional la clausura/bloqueo preventivo de la web https://drive.www.uber.com/argentina y las plataformas digitales, aplicaciones y todo otro recurso tecnológico que permitiera contratar y/o hacer uso de los servicios de transporte de pasajeros que ofrece la empresa UBER TECHNOLOGIES INC, UBER ARGENTINA SRL o UBER B.V., hasta tanto cesaran los motivos que habían dado origen a dicha medida…

2. En el recurso de inconstitucionalidad, la defensa sostuvo que la decisión confirmada por el tribunal de alzada debía equipararse a una definitiva porque había

ordenado el bloqueo de la aplicación de Uber sine die en una instancia muy previa al fallo final y ello importaría la paralización absoluta de toda actividad eventualmente comercial e impediría la comunicación entre los usuarios de la página.

Alegó gravedad institucional por violar el régimen federal, porque la decisión impugnada, al extender el bloqueo de la página web al país, excedía los límites territoriales del fuero contravencional, afectaba el régimen federal (arts. 1, 5, 121 y 129 de la CN) y violaba estándares internacionales de libertad de expresión (art. 13, inc. 1º de la CADH y "Declaración Conjunta sobre libertad de expresión e internet" de los relatores de libertad de expresión de la ONU, OEA y otros", del año 2011).

Por último, la Defensa señaló que lo resuelto se apartaba sin fundamento de la resolución anterior emitida por la misma Sala, donde se había confirmado el rechazo de la extensión del bloqueo.

3. La Sala II declaró inadmisible el recurso interpuesto considerando que la medida cautelar confirmada no causaba estado ni un agravio actual de imposible subsanación ulterior y que en la presentación no se articulaba caso constitucional alguno, sino que reeditaban cuestiones que habían sido debidamente examinadas y respondidas en el decisorio impugnado (fs. 61/63).

4. El Fiscal General a cargo, al tomar intervención, opinó que no debía hacerse lugar a la queja por falta de sentencia definitiva y de gravedad institucional (fs. 158/160).

Fundamentos:

El juez Luis Francisco Lozano dijo:

1. La decisión recurrida dispuso la "… CLAUSURA/BLOQUEO PREVENTIVO en los términos del art. 29 de la ley 12, de la página web http://drive.www.uber.com/argentina y las plataformas digitales, aplicaciones y todo otro recurso tecnológico que permita contratar y/o hacer uso de los servicios de transporte de pasajeros que ofrece la empresa UBER TECHNOLOGIES INC, UBER ARGENTINA SRA o UBER B.V., en todo el territorio de la República Argentina; hasta tanto cesen los motivos que dieran origen a la presente medida" (cf. fs. 144/147, el subrayado no pertenece al original, la mayúscula sí).

Esa decisión extendió los alcances de una anterior que había bloqueado la mencionada página para el ámbito de la Ciudad. El incumplimiento de esa medida fue la razón que la Cámara expuso para extender el "bloqueo" a todo el país.

2. La resolución descripta viene recurrida por Mariano Otero, a quien la Cámara

identificó como un "directivo" de UBER e "imputado" en estas actuaciones. La calidad de parte del recurrente no viene debatida razón por la cual no corresponde al Tribunal avanzar sobre ese extremo.

Mariano Otero cuestiona, con diversos agravios (cf. el punto 2 de las "Resulta"), la extensión nacional acordada a la medida decretada en autos. Sostiene que "… es puntualmente grave el exceso de jurisdicción en que incurrió el Poder Judicial de la Ciudad de Buenos Aires ordenando, abiertamente, una medida a ser ejecutada en todo el territorio de la República Argentina, afectando el régimen federal establecido por la Constitución Nacional en diversos artículos y contradiciendo abiertamente, sin ningún fundamento, sus propios precedentes. En este recurso se está poniendo en tela de juicio, entonces, cuestiones vinculadas al régimen federal de gobierno y la autonomía de las jurisdicciones locales, las provincias y hasta los municipios (arts. 1, 5, 121 y 129 —entre otros— de la Constitución Nacional y art. 8 de la Constitución local) y la jurisdicción federal (art. 75 inc. 13 de la Constitución Nacional), de modo que, claramente, la materia del juicio excede el interés de las partes (sea el Ministerio Público Fiscal y el imputado), y se proyecta a toda la comunidad"…

3. El perjuicio del que da cuenta el planteo descripto lleva a equiparar a definitiva a la decisión recurrida, en tanto no es uno de aquellos que pueda verse subsanado con la definitiva. Cualquiera sea el resultado final al que se arribe, éste carecerá de la virtualidad de reparar la intromisión en ámbitos que le son ajenos.

Por lo demás, si bien la decisión recurrida viene discutida desde el ángulo de lo que las normas federales invocadas disponen, lo cierto es que se encuentra, primeramente, en oposición a los límites que la misma CCBA, en su artículo 8, le acuerda a la Ciudad y dentro de los cuales operan los poderes instituidos por dicho cuerpo normativo y por las leyes de organización judicial dictadas en su consecuencia. Por ello, corresponde a este Tribunal su tratamiento (cf. el art. 113 inc. 3 de la CCBA).

4. En efecto, asiste razón a la defensa. Los jueces de mérito han excedido el ámbito de las competencias que le son propias al decretar una cautelar que excede el ámbito de la Ciudad (cf. el art. 8 de la CCBA) hasta abarcar otras jurisdicciones. Puesto en otros términos, la decisión recurrida avanza ilegítimamente sobre competencias que ni la CCBA ni la ley les acuerda.

5. Sobre esa base, corresponde revocar la extensión que la resolución recurrida le dio a clausura preventiva de la página web http://drive.www.uber.com/argentina.

6. No ha sido pedido que la mencionada clausura fuera enervada en lo que hace al ámbito de la Ciudad, razón por la cual no corresponde a este Tribunal ingresar a analizar su legitimidad. Sin perjuicio de ello, vale recordar que el art. 29 de la ley nº 12 requiere para el dictado de la medida allí prevista que una conducta que, prima facie, constituye una "contravención", ponga en "inminente peligro la salud o seguridad pública". La medida (clausura) tiene que estar limitada al "… ámbito estrictamente necesario" y su propósito se agota una vez que se "… reparen las causas [, los mencionados peligros,] que dieron motivo a dicha medida"1.

De generarse en el futuro algún debate en torno al mantenimiento de la mencionada cautelar, la decisión a su respecto deberá comenzar por establecer si están reunidos en el sub lite los reseñados requisitos a cuya verificación el legislador ha supeditado la posibilidad de dictar la medida a que se refiere el citado art. 29 de la ley nº 12.

Por ello, voto por: hacer lugar a la queja y al recurso de inconstitucionalidad; y, revocar la decisión de Cámara en cuanto fue materia de agravio.

Los jueces José Osvaldo Casás e Inés M. Weinberg dijeron:

Adherimos a los puntos 1 al 5 del voto de nuestro colega preopinante, Dr. Luis Francisco Lozano.

Por ello, votamos por: hacer lugar al recurso de queja y de inconstitucionalidad y revocar la decisión de Cámara en cuanto fue materia de agravio.

La jueza Ana María Conde dijo:

1. Coincido, en lo sustancial, con los desarrollos contenidos en el voto del juez Luis Francisco Lozano toda vez que la medida precautoria acordada en las presentes actuaciones excede el ámbito de las potestades que le han sido reconocidas a los magistrados de la Ciudad en esta materia e invade de un modo arbitrario el de otras jurisdicciones.

Concretamente, aunque las decisiones relativas a medidas cautelares no reúnen por regla el carácter de sentencia definitiva, a los fines de habilitar su tratamiento por la vía intentada (de conformidad con la constante doctrina del Tribunal y de la CSJN), corresponde hacer una excepción a ese principio general cuando como suce-

[1] Cuando el juez o jueza verifica que la contravención pone en inminente peligro la salud o seguridad pública, puede ordenar la clausura preventiva del lugar, limitándola al ámbito estrictamente necesario, hasta que se reparen las causas que dieron motivo a dicha medida, y sin que ello impida la realización de los trabajos necesarios para la reparación. // La medida es apelable sin efecto suspensivo. La Cámara, previa vista al o la Fiscal, debe expedirse dentro de la cuarenta y ocho (48) horas.

de en esta causa se explica fundadamente que la medida resistida es susceptible de originar un perjuicio que, por su magnitud y características, resulta de insuficiente o imposible reparación posterior.

Esta instancia, frente a discusiones como la suscitada en esta causa, usualmente aspira a ser prudente a la hora de anticipar su injerencia acerca de pronunciamientos no definitivos vinculados con medidas precautorias (ya sea que las decidan, mantengan o denieguen) y únicamente ha reconocido excepciones a la regla cuando se esgrimieron con contundencia motivos que aconsejaron realizarlas. Pienso que esa situación se configura en autos toda vez que la medida cuestionada por el recurrente procura tener efectos fuera de los límites de la Ciudad (arts. 8, CCABA y 8, ley nº 7) sin razón suficiente, ni excepcional alguna, que justifique ratificar un bloqueo absoluto —aunque provisorio— de una página web en toda la República, rebasando largamente el interés de la CABA en la adopción de un temperamento tan extremo en el marco de una investigación contravencional y comprometiendo de ese modo al de toda la comunidad. En el caso se investiga la conducta que esa firma y sus integrantes en principio organizan en el espacio público de esta urbe, sin la correspondiente habilitación local y omitiendo las advertencias que le han sido dirigidas; comportamiento que, aun cuando la operatoria fuese irregular, no parece capaz de vilipendiar de cara a su propia naturaleza jurídica ningún derecho de tal relevancia que autorice una limitación cautelar con el alcance pretendido.

Al respecto, por regla toda medida cautelar y en general toda decisión jurisdiccional que pronuncia un magistrado local en materia contravencional se encuentra destinada a surtir efectos esencialmente dentro del territorio de la CABA en cuyo ámbito geográfico la Constitución local le atribuye de forma exclusiva a sus tribunales la competencia para investigar y juzgar conductas que suceden o que producen sus efectos en ella (según cláusula transitoria decimosegunda, apartado quinto, CCABA; y art. 2, CC). Las Provincias (y la Ciudad) han delegado a la Nación la facultad de dictar los códigos comunes, que son de aplicación con igual alcance en todo el territorio del país, en cuyo cumplimiento está involucrado el orden público (art. 75.12, CN); y también la de sancionar las normas generales para toda la República en cuyo marco se encuentran —entre muchísimas otras— las leyes nº 26.032 y 27.078, siendo indispensable reconocer su supremacía y consecuentemente abstenerse de emitir decisiones que solapadamente las contradigan (art. 31, CN).

Considero que el bloqueo de una página web como el que fue emitido en esta causa

con proyección en todo el territorio argentino, argumentado en la inviabilidad técnica de limitarlo a un espacio más acotado y cuya eventual repercusión dependiendo de cómo sea realizado podría incluso traspasar las fronteras de la Nación —al reunir efectos extraterritoriales—, es una decisión susceptible de entrar en contradicción con los principios que cabe extraer de las normas mencionadas en último término, sin que pueda conjeturarse en el caso a su respecto un interés en principio genuino por parte de la Ciudad de hacer cesar cautelarmente la comisión de una conducta o sus efectos con la finalidad de impedir males mayores o la impunidad de sus partícipes. Es que una medida precautoria irrestricta, como la decidida, lesionaría innecesaria y desproporcionadamente derechos que allí han sido reconocidos, tales como: el acceso e intercambio de información (en tanto elementos constitutivos de la libertad de expresión, que en nuestro ámbito tiene especial protección por normas constitucionales y convencionales); la obtención de conocimientos y transmisión de ellos mediante la utilización de contenidos, herramientas y de aplicaciones; y la posibilidad de cualquier usuario de esa red global (internet) de comunicarse o desenvolverse libremente en ella.

En efecto, aun cuando en este caso hipotéticamente se considere que el comportamiento investigado incumple una serie no menor de obligaciones exigibles en la Ciudad eficaces para fundar una cautelar contravencional, lo cierto es que no le concierne a los magistrados locales decidir que análogos incumplimientos concurren, ocurren o producen efectos en todos los ámbitos geográficos en los que pretenden hacer valer esa limitación. Esta restricción, dirigida en especial contra la firma que gestiona la página e indirectamente a los habitantes de la República con el fin de impedir que puedan ingresar a la URL (o manipulen "las plataformas digitales, aplicaciones y todo otro recurso tecnológico que permita contratar y/o hacer uso de los servicios" que la firma UBER Argentina SRL según se afirma le ofrece al público sin licencia alguna —conforme fue resuelto por la instancia inferior a fs. 144/147—), se muestra inadmisible. Semejante determinación precautoria o cautelar pone en riesgo el "derecho humano a las comunicaciones" a través de internet (art. 2, ley nº 27.078), mediante la "búsqueda, recepción y difusión de información (…) de toda índole" (art. 1, ley nº 26.032); y —fundamentalmente— el principio de la "completa neutralidad de las redes" que se encuentra asegurado por nuestro ordenamiento jurídico (arts. 1, 56 y 57, ley nº 27.078).

El principio referenciado promueve en líneas generales que la libertad de acceso y elección de los usuarios para manipular, enviar, recibir u ofrecer cualquier conteni-

do, aplicación o servicio mediante internet no se encuentre condicionada o restringida por medio de bloqueos, suspensiones, filtraciones u obstrucciones sino como ultima ratio y solamente para la prevención de un acto —o conducta— que desconozca otros derechos fundamentales, previo a una ponderación adecuada, prudente y razonable de cada interés legítimo que entra en conflicto con la adopción de una medida de tal especie; interés legítimo que no se muestra posible predicar respecto de una mera conducta contravencional que conmueve en todo caso la convivencia de los porteños, al estar vinculada con el ordenamiento del espacio público de la Ciudad y de las actividades lucrativas que en ella se ofrecen, pero puede no afligir a la de sus vecinos con igual o similar alcance. Lo aquí decidido no importa abrir un juicio con relación a la conveniencia o inconveniencia de avalar una medida cautelar en el limitado ámbito de la Ciudad con el propósito de que no sigan produciéndose efectos de una conducta al parecer vedada (aunque ello sea impracticable a nivel informático); ni inhibiría a los involucrados debidamente informados de una restricción de aquella especie a que evidencien su mayor esfuerzo por respetarla y por corregir las razones que pudieron haberle dado fundamento, o bien —en el escenario de no hacerlo, de manera deliberada y consciente, desconociendo las eventuales exhortaciones dirigidas— resulten responsabilizados contravencionalmente de cara a sus inobservancias como el ordenamiento citadino lo permite.

2. En mérito a lo expuesto, corresponde hacer lugar a la queja, admitir el recurso de inconstitucionalidad y revocar el pronunciamiento de la Sala II de la Cámara de Apelaciones en lo PCyF, en cuanto fue materia de agravio.

Así lo voto.

Por ello, y habiendo tomado la intervención que compete al Fiscal General a cargo, el Tribunal Superior de Justicia resuelve:

1. Hacer lugar al recurso de queja interpuesto.

2. Hacer lugar al recurso de inconstitucionalidad y revocar la resolución de la Sala II de la Cámara de Apelaciones en lo Penal, Contravencional y de Faltas de fecha 04/04/2017, en cuanto fue materia de agravio.

3. Mandar que se registre, se notifique y, oportunamente, se remitan las actuaciones a la Cámara de Apelaciones en lo Penal, Contravencional y de Faltas.

La jueza Alicia E. C. Ruiz no firma por encontrarse en uso de licencia.

Caso Organización Veraz *versus* Open Discovery

Derecho de marcas. Uso de marcas como keywords en buscadores de Internet para generar publicidad. Marca notoria. Aprovechamiento del prestigio ajeno. Responsabilidad civil. Daños. Forma de valuar el daño. Responsabilidad del competidor que usa una marca notoria.

Causa nº 1789/09. "Organización Veraz SA C/ Open Discovery"

En Buenos Aires, a los 4 días del mes de mayo del año dos mil dieciocho, hallándose reunidos en acuerdo los Señores Vocales de la Sala III de la Excma. Cámara Nacional de Apelaciones en lo Civil y Comercial Federal a fin de pronunciarse en los autos "Organización Veraz SA C/ Open Discovery SA S/ Cese de Uso de Marca", y de acuerdo al orden de sorteo la doctora Graciela Medina dijo:

I. Mediante el pronunciamiento dictado a fs. 2214/2217, el magistrado de primera instancia hizo lugar a la demanda entablada por Organización Veraz SA, y en consecuencia, condenó a Open Discovery SA", a cesar en el uso de las marcas "VERAZ" y "ORGANIZACIÓN VERAZ" así como de otros signos confundibles con las marca de la actora como "VERAS"; "BERAZ" o "BERAS" y a pagarle a aquella en el plazo de diez días la suma de pesos treinta y cinco mil ($35.000) con más los respectivos intereses. A su vez, le impuso a la vencida las costas del pleito y la publicación de la sentencia en los términos del artículo 34 de la ley 22.362.

Para así decidir, puso de resalto en primer término que las marcas de la actora "VERAZ" y "ORGANIZACIÓN VERAZ" son marcas notorias, toda vez que son conocidas más allá de la rama comercial en la que se desarrollan y son identificadas con un producto o servicio determinado. En tal sentido, señaló que cuando de marcas notorias de trata, debe hacerse un análisis riguroso del caso pues debe evitarse el aprovechamiento del prestigio ajeno y hacer prevalecer la lealtad y la buena fe comercial conjurando confusiones que sólo pueden beneficiar a quienes transgreden dichos principios.

Por otro lado, tuvo en cuenta que en las actuaciones quedó acreditado que la demandada contrató el servicio de enlaces patrocinados "Adwords" de Google, utilizando como palabra clave la marca de la actora "VERAZ" (Conf. informe de fs. 1316/1321). También corroboró que del informe elaborado por el perito informático designado en autos (ver fs. 1691/1711) surgía que al insertar en el buscador de Google las palabras "VERAS"; "BERAZ"

o “BERAS”, aparecía la publicación de la accionada.

Sentado ello, el juez consideró que esta última utilizó los términos “VERAZ” y “ORGANIZACIÓN VERAZ” como palabras clave para derivar —en su búsqueda— a los usuarios de www.google.com.ar hacia su sitio web, con la finalidad comercial de captar clientela para operar e interactuar en su propia plataforma on line. Indicó que la contratación de estos servicios de “keywords” o enlaces privilegiados revela una intencionalidad de la accionada de beneficiarse con la utilización de la marca ajena. Sostuvo que se produce así una asociación ideativa —en los consumidores— entre los servicios de Organización Veraz y de Open Discovery por la utilización como “palabra clave” de la marca notoria de la actora.

Concluyó que esta asociación causa un daño al titular de la marca en razón de la confusión provocada a través del signo notorio. Así, tuvo por acreditado el uso indebido por parte de la demandada de las marcas de la actora y condenó a ésta última al cese de uso de las mismas.

Por último, formuló un análisis de los daños alegados por la accionante, ponderando que toda infracción marcaria produce un daño que debe ser resarcido a fin de evitar que quien comete la conducta ilícita permanezca impune y que, en el caso, resultaba evidente que la accionada quiso aprovechar el prestigio de la parte actora y que su conducta (ilícita) conduce a la dilución de la marca en cuestión y a la confusión de la clientela.

Teniendo en cuenta ello y haciendo uso de la facultad que le otorga el artículo 165 del Código Procesal, estimó los daños reclamados en la suma de $35.000 […]

II. La parte actora se agravia por entender que la indemnización concedida por el a quo en concepto de daños y perjuicios ocasionados por la infracción marcaria es muy exigua si se tiene en cuenta el monto que surge de la prueba producida en el expediente, que tiene como piso la suma de $3.336.468 estimada por el perito contador designado en autos. También se queja porque —según sostiene— el juez omitió considerar que la demandada incurrió en competencia desleal.

La demandada se agravia de la sentencia apelada en los siguientes términos, a saber: 1) el carácter genérico en que habría decantado la marca “VERAZ” en tanto sinónimo de informe comercial, lo que descarta de plano que sea una marca notoria; 2) que la marca de la actora es un signo débil por cuanto se trata de una palabra de uso común altamente descriptiva del

producto al que se la asocia; 3) la inexistencia absoluta de productos, avisos o servicios suyos en los que se haya exhibido la marca de la actora y la inexistencia de confusión por parte de los consumidores y 4) no existe infracción marcaria al utilizar una marca ajena como "palabra clave" en el sistema Adwords de Google, en la medida que no se ofrezcan meras imitaciones de productos y que dicho uso no menoscabe la funciones de la marca del competidor. Por último, tilda la sentencia de arbitraria.

III. Así reseñada la causa en los aspectos sustanciales que interesan en esta instancia, y antes de entrar al estudio de las cuestiones traídas a esta Alzada, que juzgo necesarias frente al tenor de los agravios; señalo que no he de seguir a las apelantes en todos y cada uno de sus planteamientos, limitándome en el caso, a tratar sólo aquéllas que son "conducentes" para la correcta adjudicación de los derechos que les asisten. […]

A lo que debo añadir que: a) examinaré cada cuestión —hechos, pruebas y fundamentos— de manera que nada que sea sustancial quede sin tratar; b) intentaré ser concisa, por motivos de claridad para sustentar la decisión; bien entendido que he valorado todas las pruebas y reflexionado sobre todos los argumentos expuestos por las partes […]

V. Despejado este aspecto tangencial del caso, vayamos pues al tema de fondo.

Lo que se discute en los presentes obrados es **si la utilización por parte de la demandada de las marcas de la actora (ambos competidores) como palabra clave "keyword" en el sistema de enlaces patrocinados o "keyword advertising" de los distintos buscadores en internet —en el caso Google AdWords— constituye una infracción marcaria en los términos de la ley 22.362 y un acto de competencia desleal** tal como lo plantea la actora en el escrito de inicio.

Teniendo en cuenta la novedad de la cuestión aquí planteada, resulta necesario explicar en qué consiste y cómo funciona dicho sistema.

La búsqueda en internet a partir de una o varias palabras a través de un motor de búsqueda se ha convertido en parte de nuestra cultura. Sin embargo, resulta desconocido para la mayoría del público en general, el funcionamiento interno de cómo los resultados de estas búsqueda opera. Se asume simplemente que si un usuario de internet teclea ciertas palabras que considera importantes para su búsqueda, aparecerá la información que desea.

Así, al aparecer los resultados de las búsquedas, nos encontramos también con

pequeños anuncios en forma de ventanas que contienen publicidad y que son a su vez hipervínculos a las páginas Web de los anunciantes, de manera tal que si el usuario hace clic en los mismos será llevado a estas páginas (enlaces patrocinados).

Cabe destacar que se advierten dos tipos de resultados en las búsquedas de los usuarios. Los primeros, son los denominados resultados "orgánicos" o "naturales", que se originan cuando un usuario efectúa una búsqueda a partir de una o varias palabras y el motor de búsqueda muestra los sitios que parecen ajustarse más a dichas palabras por orden decreciente de pertinencia en relación con la información solicitada. Los segundos, son aquéllos derivados de un servicio remunerado como es el caso de Google Adwords también denominado Cost-Per-Click (CPC) Internet Advertising Model Like Adwords. Este servicio permite a los operadores económicos seleccionar una o varias keywords para que, en el caso de que coincidan con las palabras introducidas en el motor de búsqueda, se muestre un enlace promocional de su sitio. Dicho enlace aparece bajo la rúbrica "enlaces patrocinados", que se muestra generalmente en la parte derecha de la pantalla, a un lado de los resultados naturales, o bien en la parte superior de la pantalla, justo encima de dichos resultados. De tal forma que el sistema, en su conjunto, funciona como mecanismo de promoción publicitaria, actuando los enlaces patrocinados como anuncios asociados a las palabas claves introducidas por los usuarios en el motor de búsqueda.

Las empresas con presencia en internet, en su intento por atraer visitas a sus páginas web, encuentran en este un atractivo medio publicitario, además de un fabuloso instrumento de atracción de clientela y una significativa fuente de ingresos, pues cuantas más visitas tenga una página web, más conocida será y más se pagará por espacio publicitario (Mónica Lastiri Santiago, "El tratamiento jurídico de las Keywords Advertising en la jurisprudencia del Tribunal de Justicia de la Unión Europea", *IUS Revista del Instituto de Ciencias Jurídicas de Puebla*, México, ISSN: 1870-2147. Año VII Nº 31, Enero-Junio de 2013, pp. 167-182).

Indudablemente, la aparición de internet en el mundo de los negocios ha cambiado la naturaleza de la publicidad. Hoy, las empresas pueden dirigirse a audiencias específicas basándose en las Keywords Advertising.

Actualmente, es evidente que el servicio o motor de búsqueda de Google es el sistema de publicidad más popular en internet, y ofrece una serie de enlaces a sitios

en línea a partir de uno o varios términos clave introducidos por el usuario del servicio denominado AdWords.

A través de su servicio de referenciación, Google comercializa palabras clave que pueden ser seleccionadas por varios operadores para después ofrecer un servicio de almacenamiento y puesta a disposición de enlaces patrocinados acompañados de un breve mensaje comercial elaborado e insertado en el sistema por el anunciante que "adquiere" la palabra clave de Google. El anunciante puede mejorar su lugar en el orden de aparición en cualquier momento fijando un precio máximo por click más elevado o intentando mejorar la calidad de su anuncio. Vale destacar que el sistema funciona en forma automática, pues los anunciantes que se sirven de este servicio remunerado seleccionan las palabras clave, redactan la comunicación comercial e insertan el enlace (link) promocional a su sitio web.

Aunque suene redundante, conviene poner de resalto que las empresas interesadas en que su página aparezca en los primeros lugares de los enlaces patrocinados, y lograr de esta manera publicitar sus productos pueden —contratando con el buscador el programa AdWords— escoger una serie de palabras claves o keywords para que el link a su página web aparezca en los resultados de una búsqueda que incluyó todas o algunas de las palabras claves escogidas por el anunciante. El mayor o menor posicionamiento que logrará el anunciante en los resultados patrocinados estará dado por el precio que está dispuesto a pagar por cada click que recibe, mediante un sistema de subasta. De modo que, mientras más anunciantes están dispuestos a contratar esa palabra clave, más elevado será el costo por click (Porthé, Luis Ignacio, "Referencias a marcas ajenas en las campañas publicitarias en buscadores de internet. Implicancias a la luz de las normas marcarias, de lealtad comercial, de defensa del consumidor y de defensa de la competencia, publicado en: DCCyE 2013 (octubre), 01/10/2013, 287, Cita Online: AR/DOC/1235/2013).

A modo de ejemplo, podríamos imaginar la situación en que Adidas elige como keyword o palabra clave el término "Nike" —una competidora— con el fin de publicitar un nuevo par de zapatillas que lanza al mercado. Así, sucedería que cada vez que un internauta ingresara el término "Nike" al motor de búsqueda, encontraría entre los primeros resultados de la búsqueda enlaces promocionales al sitio oficial de Adidas o de negocios que venden ese producto que la firma pretende publicitar.

Tal como ha sido dicho en el primero de los artículos que he citado en los párrafos precedentes, la publicidad contextual es

una modalidad de alta segmentación que se considera poco intrusiva, pues se dirige a un público que se sabe, de antemano, está interesado en un producto o servicio determinado. Sin embargo, este tipo de publicidad representa uno de los muchos problemas que tienen los titulares de marcas en el entorno digital, pues desde la perspectiva del derecho de marcas, numerosos operadores económicos cuestionan la legalidad de la publicidad en los motores de búsqueda en internet utilizando determinadas palabras clave.

En tal contexto, surge como interrogante si bajo la sombra de nuestro ordenamiento marcario puede un anunciante basarse en una referencia a una marca ajena para promocionar sus productos, y si dado el caso, existe o no un uso indebido de marca.

Lo cierto es que resulta muy escasa la jurisprudencia de nuestros tribunales sobre este tema puntual y, tal como lo han manifestado las partes al expresar agravios, resulta útil recurrir a la lectura de los precedentes de otros países a fin de nutrir el análisis, aunque sin perder de vista que no existe en éstos uniformidad absoluta de criterios y que nuestra legislación sobre la cuestión difiere sustancialmente con la de otros países. No obstante ello —según mi criterio— la cuestión que aquí se discute encuentra acabada respuesta en la legislación actual de nuestro país.

En nuestra doctrina, están quienes sostienen que en lo referente a keywords, no hay uso que provoque confusión pues no hay ilegalidad en el uso de lo que no es visible para el público. Aducen que se utiliza la marca ajena como palabra clave con el único objeto de lograr el posicionamiento de su negocio en las redes pero sin la menor posibilidad de generar confusión en el público consumidor pues éste jamás se entera de dicha utilización. Por lo demás, señalan que los enlaces patrocinados aparecen en un sector determinado de la búsqueda, fácilmente distinguibles de los resultados "naturales" que arroja la misma y que en definitiva será el internauta quien libremente decida a qué sitio ingresar (ver "Ley de Marcas, Metatags y keywords", Jorge Otamendi, *LL* 2012-B, 1178 y artículo ya citado del Dr. Porthé, Luis Ignacio, entre otros).

Cabe destacar que en defensa de dicha tesis, se utiliza como ejemplo el caso de la publicidad por carteles en determinados lugares, indicando que más allá de la mecánica y el medio en que se hará la publicidad, se trata de adquirir presencia con publicidad paga o simplemente con el sitio en una página, y cerca de las marcas líderes. Sostienen que esto no tiene nada de ilegal y es lo que se conoce como competencia. Por otro lado, señalan que al realizar la búsqueda, el internauta tendrá ante sí una cantidad de vínculos y decidirá entre

ellos en cuál hacer click y que tal situación resulta equiparable a la de quien ingresa a un supermercado con la idea fija de comprar un producto determinado pero cambia de opinión al encontrar en la góndola otro producto de similares características y calidad pero con mejor precio. No existe en ello nada de ilegal.

En cambio, en la vereda de en frente, hay autores que sostienen que la selección por parte de un competidor de una marca ajena como palabra clave en un sistema de publicidad por enlaces patrocinados constituye una infracción marcaria (Papaño Javier "Usos de marcas como palabras clave (keywords)", en XXIV Jornadas Anuales de Propiedad Intelectual de la AAAPI, 26 y 27/8/2010, Buenos Aires, Argentina).

En defensa de su postura indican que la confusión y/o posibilidad de confusión en el consumidor es concreta y que una prueba fehaciente en este sentido puede ser la cantidad de clicks que registra el buscador luego de imprimir el aviso competidor que paga por usar la marca ajena. Otro indicio es que los programas de sugerencias de palabras incluidos en el sistema de publicidad se basan en identificar cuáles son las palabras más buscadas y elegidas, justamente, pues ello lleva a un mayor tráfico hacia el sitio del anunciante y contribuye al incremento de las ventas (Rizzo Jurado, Marco, "Uso de marcas ajenas en internet. Publicidad referencial y disparadores de nuevos desafíos", Cita Online: AP/DOC/4358/2012).

Tal como mencioné, ambas partes han citado jurisprudencia internacional sobre el tema en discusión. Al respecto, y sólo a modo de soporte doctrinario, haré una veloz y breve reseña de los criterios que sobre el particular han vertido tanto la jurisprudencia norteamericana como la europea.

En Estados Unidos de América, la jurisprudencia sobre el uso de marcas en los buscadores se vio dividida en un principio pero hoy son mayoritarios los pronunciamientos que consideran el uso de una marca ajena como keyword como un "uso en el comercio", considerando que tal conducta configura una posible infracción marcaria.

Así, en la causa "800-Cigar Inc. vs. GoTo.com" la Corte del distrito de New jersey, con fecha 13.7.2006, concluyó que la demandada realizó un uso de marca ajena en el comercio. Fundamentó su posición en que GoTo obtuvo un beneficio sobre el valor de las marcas de la actora y que, mediante su programa de sugerencias de resultados de búsqueda (el cual listaba los términos más buscados), recomendó implícitamente a los anunciantes la elección de marcas del actor como keywords.

Me interesa destacar lo decidido en el caso "J.G. Wentworth, S.S.C. Limited Parternship vs. Settlement Funding LLC Peachtree Settlement Funding" (Caso 2:06-cv-00597/-TON, Corte del distrito de Pennsylvania, 1/42007). La actora demandó a la accionada por infracción a la Lanham Act y por competencia desleal, alegando el uso por parte de ésta de las marcas registradas "J.G. Wentworth" y "JG Wentworth" como keywords en el sistema de Google Adwords (ambas empresas prestaban el mismo tipo de servicio). En este caso, la Corte rechazó la defensa de la demandada y concluyó que el uso de una marca ajena como keyword es un uso "en el comercio" que implica un ilícito marcario, conforme los términos del artículo 32 de la Lanham Act. En tal sentido, sostuvo que dicho uso no es análogo al uso interno alegado por el demandado y que se había cruzado la línea del uso interno al uso en el comercio bajo los términos de la Lanham Act.

Respecto de los precedentes en Europa, cabe destacar que si bien el Tribunal de Justicia de la Unión Europea (TJUE) ya se ha expedido en varios casos sobre esta cuestión (Google France vs. Louis Vuitton Malletier SA y expedientes acumulados, asuntos C-236/08, C-237/08 y C-238/08, con fecha 23/10/2010, entre otros), me interesa apuntar las conclusiones a las que arribó en el caso "Interflora Inc. Interflora British Unit vs. Marks & Spencer plc Flower Direct Online Limited" del 22/9/2011. Aquí, el TJUE reafirmó que la selección de una marca ajena como palabra clave por un competidor en el marco de un servicio remunerado de referenciación constituye "uso en el tráfico económico" por parte del anunciante en los términos de la normativa comunitaria. Ello, por cuanto este uso se realiza en el contexto de una actividad comercial con ánimo de lucro y no en la esfera privada. Recordó que existe un uso para "productos o servicios" incluso cuando el signo elegido como palabra clave no sea visible, es decir, aun cuando no aparezca en el anuncio patrocinado (tanto en el enlace como en el mensaje comercial).

Aquí, el TJUE mantuvo la posición adoptada en otros fallos ("Google France", "BergSpechte", "Portakabin" y "L'oreal, entre otros) en cuanto a que el titular de la marca estará facultado a prohibir a su competidor dicho uso en tanto éste pueda producir un efecto adverso en alguna de las funciones de la marca.

La novedad de en este fallo y que resulta útil para el análisis del presente, reside en el tratamiento jurídico de las Keywords Advertising que da el TJUE en lo referido al alcance de la protección conferida a los titulares de marcas de renombre. Al respecto, brinda dos elementos que habrán de tomarse en

cuenta para conocer en qué circunstancias procede considerar que un anunciante que haga aparecer un vínculo promocional hacia su sitio web a partir de un signo idéntico a una marca de renombre que ha seleccionado sin el consentimiento del titular de esta marca en el marco de un servicio de referenciación en internet es un uso que menoscaba el carácter distintivo o notoriedad de la marca, o se aprovecha indebidamente de ese carácter distintivo o notoriedad de la marca. Dichos elementos son la dilución de la marca y el parasitismo. La dilución, consiste en la disminución de la capacidad distintiva de una marca notoria para distinguir productos o servicios, sin importar la presencia o ausencia de: 1) competencia entre el propietario de una marca notoria y otros terceros, y 2) probabilidad de confusión, error o engaño. El TJUE define el parasitismo como el provecho obtenido indebidamente del carácter distintivo o de la notoriedad de la marca. Esta noción no se vincula al perjuicio sufrido por la marca, sino a la ventaja obtenida por el tercero del uso del signo idéntico o similar a la marca (ver artículos ya citados de Mónica Lastiri Santiago y Rizzo Jurado, Marco).

Ahora bien, hecho ya el recorrido por la jurisprudencia de Estado Unidos de América y Europa, considero necesario expedirme respecto de una cuestión que —con alguna confusión— plantea la demandada en su expresión de agravios, a saber: ¿Es la marca de la actora una marca notoria o es una marca genérica?

Por designación genérica se tiene a aquéllas marcas que resultan irregistrables pues se trata, como su nombre lo indica, de designaciones que definen no directamente el objeto en causa, sino la categoría la especie o el género, a los que pertenece ese objeto. Es el caso de palabras tales como "Automotor", "Motor", "Máquina", "Mueble", "Asiento", entre tantos. No puede pretenderse un privilegio sobre estas palabras (Jorge Otamendi, *Derecho de Marcas*, Novena edición actualizada y ampliada, Ed. Abeledo Perrot, pág. 75).

¿Puede alguien razonablemente creer que las marcas "Organización Veraz" o "Veraz" son marcas genéricas? La respuesta es obvia: NO. De hecho es evidente que ambas son marcas notorias.

La notoriedad es un grado superior al que llegan pocas marcas. Es una aspiración que los titulares marcarios siempre tienen. El lograr ese status implica un nivel de aceptación por parte del público que sólo es consecuencia del éxito que ha tenido el producto o servicio que las marcas distinguen. Respecto de la notoriedad de una marca, corresponde señalar que la misma funciona como factor de distinción. Cabe recordar que para que exista, la marca debe ser reco-

nocida por la mayor parte del público, sea consumidor o no del producto. La marca notoria es conocida por casi la totalidad del público. Trasciende la rama comercial o industrial en la que se encuentra. Este conocimiento no basta, hace falta el segundo requisito, que la marca sea identificada con un producto o servicio determinado. Su sola mención debe provocar esa inmediata asociación. (Jorge Otamendi, *Derecho de Marcas*, Novena edición actualizada y ampliada, Capítulo VIII, págs. 443 y sigs., Ed. Abeledo Perrot).

Sin lugar a dudas, el símbolo de la actora reúne los requisitos apuntados en el párrafo precedente ya que el público consumidor asocia el término "VERAZ" al famoso informe crediticio.

Nótese que según la accionada la marca de la actora habría decantado en designación genérica en tanto "VERAZ" es sinónimo de informe comercial. Se advierte en dicha aseveración la confusión propia de quien navega sin brújula por las aguas del derecho marcario. En efecto, si la marca "VERAZ" se ha transformado hoy en sinónimo de informe comercial o crediticio, lo es por haber adquirido luego de muchos años el carácter de marca notoria. En tal sentido, considero importante resaltar que la designación "VERAZ" no remite a la idea de informe comercial o crediticio en general sino puntualmente y especialmente al servicio que presta la aquí actora, vale decir que la asociación es inmediata.

Pues bien, es sabido que las marcas notorias deben ser protegidas de la dilución y del parasitismo y al respecto me remito —por razones e brevedad— a la definición brindada por el TJUE en el caso "Interflora" ya citado, que además, es conteste con lo que sostiene desde hace años la doctrina y jurisprudencia de nuestro país.

Ahora bien, luego de un análisis concienzudo del tema y de una valoración atenta de la prueba producida en la causa, resulta a todas luces evidente que la demandada ha utilizado la marca de la actora como palabra clave (keyword) en el sistema Adwords de Google, con el único fin de aprovecharse del prestigio y renombre de aquélla. En efecto, mediante este sistema la accionada se ha garantizado el acceso a una cartera de clientes con un mínimo costo de inversión y esfuerzo comercial.

Me interesa volver al ejemplo que plantea cierto sector de la doctrina referido al consumidor que va al supermercado en procura de un determinado producto pero que al advertir en la góndola varias opciones similares, se inclina por aquélla que le brinda mejor precio. Entiendo que tal supuesto no se adecúa a la realidad de las keyword advertising pues sabido es

que quien pretenda colocar su producto en la góndola de un supermercado deberá efectuar una fuerte inversión. Dicho en otros términos, no cualquiera puede colocar sus productos en la góndola de un supermercado y mucho menos en un sector preferencial de la misma.

Siguiendo con el ejemplo, es evidente que la utilización de la marca de la actora es lo que le ha permitido a la demandada acceder y posicionarse en esa "góndola" y no se ha producido ninguna prueba tendiente a demostrar lo contrario.

Por otro lado, no comparto el argumento mediante el cual algunos sostienen que limitar la utilización de keywords redundaría en un retraso en el avance del comercio electrónico, pues acotaría las posibilidades de elección de los internautas. Sostener esto es como aseverar que la exigencia de alcohol cero en los conductores y la imposición de velocidades máximas con el fin de evitar muertes por accidentes de tránsito perjudicarían gravemente la economía de la industria automotriz pues los potenciales compradores de autos dudarían mucho respecto de la conveniencia de comprar uno frente tales exigencias.

De las probanzas arrimadas a la causa surge con palmaria claridad que la demandada presta un servicio similar al de la actora lo cual la convierte en potencial competidora, y también se encuentra acreditado que ingresó al mercado con bastante posterioridad a ésta (ver informes comerciales de fs. 320/420 del incidente de medidas cautelares y estatuto agregado a fs. 1721 del presente).

En tales condiciones, y ponderando lo dicho en los párrafos que anteceden, no puede negarse que la accionada se ha aprovechado indebidamente del prestigio ajeno con el objeto de posicionarse en el mercado, incurriendo así en una infracción marcaria y en un acto de competencia desleal.

No es cierto que el internauta o potencial consumidor no vea la marca utilizada como palabra clave, de hecho, la teclea al efectuar la búsqueda y la ingresa porque es eso precisamente lo que busca. Podría alguien alegar alegremente que tal vez, lo que busca el internauta es el significado de la palabra "VERAZ" pero tal argumento se rebate fácilmente con la prueba pericial por cuanto allí puede comprobarse con absoluta precisión cuántas veces se cliquea el link de cualquiera de las partes una vez que apareció en el resultado luego de ingresado dicho término en el motor de búsqueda (ver prueba pericial informática de fs. 1691/1711, en especial punto 13).

Nada impide a un comerciante utilizar el sistema Adwords de Google (o cualquier

otro) para promocionar sus productos y colocarlos como enlaces patrocinados cerca los resultados naturales de las búsquedas en los que aparecen sus competidores, pudiendo para ello elegir entre cientos de palabras clave o keywords, pero otra cosa muy distinta es montarse sobre la marca de una competidora y aprovecharse del envión que su notoriedad brinda. Esto último es absolutamente desleal y contrario a la buena fe comercial.

No resulta ocioso remarcar que este tipo de publicidad sólo aparece en el momento oportuno en que una persona está buscando en internet algo específico y utilizando un término concreto y no cualquier otro. A modo de ejemplo, quien venda mamaderas, seguramente utilizará como palabras clave los términos: mamadera, leche, bebé, etc. Quien publicita paga por el click que hace el usuario en su link y no por la visualización del aviso.

Remitiéndome de los criterios esbozados por la jurisprudencia norteamericana y del TJUE, considero evidente que la utilización de la marca ajena como keyword (y en especial la de una competidora) configura un "uso en el comercio" o un "uso en el tráfico económico". Me valgo de estos conceptos porque la ley 22.362 ha sido dictada cuando estas cuestiones estaban más cerca de la ciencia ficción que de la realidad y para contrarrestar la opinión de aquéllos que pretenden imponer la idea de que se trata de un simple uso interno y absolutamente inocuo para la competencia.

Otro punto insoslayable en este conflicto es que la demandada ha incurrido en competencia desleal por cuanto mediante la utilización de la marca notoria de la actora ha procurado captar clientes y desviarlos en favor suyo. Insisto con remarcar que ambas compiten en el mismo mercado y que esta circunstancia es fundamental para resolver el caso. También insisto en remarcar que el link de la accionada aparecía en los primeros lugares de la búsqueda (como enlace patrocinado) justo cuando los usuarios de internet realizaban la búsqueda insertando la marca notoria de la actora.

Considero importante poner de resalto que la demandada intentó eludir de manera aviesa el cumplimiento de la medida cautelar dictada en su oportunidad mediante la utilización de las mentadas keywords en el sitio www.dateas.com, el cual, a la a luz de las pruebas acompañadas por la actora, se encuentra íntimamente ligado a globinfo (ver fs. 285/287 vta. del expediente de medidas cautelares nº 12.603/07, el cual tengo a la vista; ver respuesta de Google obrante a fs. 1320/1321; informe de fs. 1736 y pericial informática de fs. 1691/1721).

El principio de buena fe y lealtad comercial le imponía a ésta, cumplir acabadamente y en forma diligente con la cautelar … para evitar las violaciones marcarias y los daños que ellas producen al titular de una marca notoria.

Lo dicho anteriormente tiene su razón de ser en el deber de prevención que surge del artículo 19 de la Constitución Nacional y del principio de buena fe que obliga no solo a reparar el daño sino a prevenirlo.

Sobre este tema quiero aclarar que estoy convencida que la responsabilidad civil tiene dos funciones: prevención y reparación. Si bien la función preventiva no está explícitamente reconocida en el Código de Vélez se deriva del principio de buena fe y ha sido aceptada por la jurisprudencia (CSJN, 6/3/2007, RCyS, 2007- 344; LA LEY, 2007-B, 363; RCyS, 2007-344) y receptada expresamente en el Código Civil y Comercial en su artículo 1708, que dice: Funciones de la responsabilidad. Las disposiciones de este Título son aplicables a la prevención del daño y a su reparación.

En virtud del deber de prevenir el daño que se deriva del artículo 19 de la Constitución Nacional y del principio de buena fe toda persona tiene el deber, en cuanto de ella dependa, de: a) evitar causar un daño no justificado; b) adoptar, de buena fe y conforme a las circunstancias, las medidas razonables para evitar que se produzca un daño, o disminuir su magnitud (conf. art. 1710 del CC y C ley 26.994).

Así las cosas, no quedan dudas respecto de la responsabilidad que le cabe a la demandada

El fundamento de esta responsabilidad radica en las siguientes circunstancias probadas a lo largo del procedimiento:

(i) La utilización de las marcas de la actora como keywords para montarse sobre su prestigio y trayectoria y posicionarse así en los primeros resultados de la búsqueda (como enlace patrocinado).

(ii) La demandada no fue diligente en el cumplimiento de la medida cautelar oportunamente dictada y continuó con el uso de las marcas de la actora o similares.

(iii) De la prueba pericial informática obrante en autos surge de manera palmaria que la accionada se benefició utilizando las marcas notorias de la actora.

En definitiva, lo que aquí se está protegiendo es la marca notoria en sí misma, su capacidad distintiva y su unicidad y no el castigo de conductas ilícitas de terceros involucrados. En un breve paréntesis recuerdo, que esta Cámara ha mencionado, en múltiples precedentes, el efecto dañi-

no que produce la dilución de la marca notoria; esto es la gradual disminución o dispersión en cuanto al valor indicativo de la marca y demostrativa de una calidad característica (ver Sala II, causa 957/99 de septiembre 2002).

Por otro lado y a mayor abundamiento, cabe recordar que cada vez que se comete una infracción marcaria se produce el primer daño cierto al titular de la marca. Se ha dicho que en la mayoría de los casos es imposible probar que las ventas del producto original disminuyeron o que éstas dejaron de aumentar por causa de la aparición en el mercado del producto o servicio con marca en infracción. Puede haber dudas respecto de estas cuestiones, pero tal como señala Callman, "las más elementales concepciones de justicia y orden público requieren que quien actúa indebidamente correrá con el riesgo de la incertidumbre que su propio acto indebido ha creado". Una posición contraria contribuiría a la creación de un halo de impunidad alrededor de las infracciones marcarias, penales o civiles. (Conf. Jorge Otamendi, *Derecho de Marcas*, Novena ed. actualizada y ampliada, Abeledo Perrot).

No obstante lo dicho hasta aquí, me interesa poner de resalto una vez más que lo que valoro especialmente en este caso en particular es el hecho de que ambas partes prestan un servicio similar, que considero inaceptable y desleal el uso de un marca ajena como keyword.

En función de lo expuesto, considero que corresponde modificar este aspecto del fallo por cuanto corresponde agregar que además de haber cometido una infracción marcaria mediante el uso indebido de las marcas de la actora, la demandada ha incurrido en un acto de competencia desleal.

VI. El señor Magistrado, como vimos, hizo lugar al reclamo de la indemnización de los daños y perjuicios incoada por la actora por la cantidad de $35.000, que motiva —en sentido contrario— las quejas de la demandada y de la actora.

Tal como he dicho en el considerando anterior, la marca de la actora es una marca notoria o de alto renombre y muy difundida, que a la fecha de la iniciación de la demanda llevaba varios años de efectivo uso en nuestro mercado. Tal antigüedad, su explotación continuada y su difusión y propaganda justifican otorgarle una protección concorde con dichas circunstancias, particularmente expuesta a usurpaciones y en definitiva al indebido aprovechamiento de su prestigio —ganado con esfuerzo— y a su poder de convocatoria. Este tipo de marcas se encuentran contempladas en el artículo 6 bis del Convenio de París (ley 17.011).

Sobre este aspecto del litigio, cabe señalar que, frente a las notorias dificultades para la prueba del daño causado por una infracción en el ámbito de la propiedad industrial, la más moderna doctrina se ha inclinado —no sin sólidos fundamentos— por sostener que, como regla, toda infracción marcaria provoca un daño. Y como éste en general, es de difícil prueba, y la notoria dificultad que existe para probar la relación causal entre una infracción marcaria y los daños derivados de ella, los autores propician que se parta de una presunción de daño, debiendo los jueces, para superar los problemas probatorios y evitar que éstos obren como vehículos de la impunidad, recurrir a la fijación prudencial que autoriza el art. 165, última parte, del Código de rito, en función de una cautelosa apreciación de las circunstancias de cada causa …

La ilegítima conducta de quien utiliza una marca ajena para comercializar su servicio no se puede amparar en la dificultad de la prueba para eludir sus responsabilidades civiles. Por ello, frente a determinadas actitudes, suele ser razonable presumir la existencia de daños —en favor del titular del derecho conculcado— como fruto causal eficiente del ilícito, aunque de difícil prueba, pues el infractor ha causado daños ciertos y no meramente conjeturales.

Lo cierto es que en el sub examen la actora se ha preocupado por producir prueba concreta tendiente a demostrar el daño alegado. La demandada, en cambio, optó por negar todo de manera sistemática, formulando alegaciones genéricas, sin brindar herramientas concretas que permitan sostener su postura.

Sobre este aspecto, es importante remarcar la labor de la perito contadora designada de oficio, Ana María Banko, quien estimó la valuación del daño en la suma de $3.336.468, basándose para ello en los datos suministrados por Google sobre la cantidad de impresiones y clicks (ver fs. 2020/2024, fs. 2035/2035 vta. y fs. 2036).

Por su parte, la actora estimó la valuación del daño en la suma de $5.951.836.

Tal como he señalado en otra ocasión, el magistrado no puede desvincularse arbitrariamente de la opinión del experto, debiendo en todos los supuestos fundar su discrepancia en elementos de juicio que permitan desvirtuar el informe, concluyendo fehacientemente en el error o el inadecuado uso que el experto hubiera hecho de los conocimientos científicos de que su profesión o título habilitante necesariamente ha de suponerse dotado. Es que entiendo que si el órgano judicial ha considerado que para llegar a resolver el caso controvertido eran necesarios conocimientos técnicos científicos o artísticos determinados, no puede con posteriori-

dad hacer caso omiso al dictamen pericial, salvo que en la sentencia haga una valoración adecuada de la prueba razonando la ineficacia de la misma, la insuficiencia del razonamiento o la falta de claridad en las conclusiones ofrecidas. (conf. esta Sala en la causa Nº 45.424/95 de fecha 01.09.2005).

En tales condiciones, por los motivos apuntados en el párrafo que antecede, dentro del marco de dificultades que es propio del tema y valorando en conjunto las circunstancias de la causa, considero prudente modificar este aspecto de la sentencia y fijar la valuación del daño en la suma de $ 3.336.468 estimada por la perito contadora designada en autos (conf. artículo 165, última parte del Código Procesal).

La suma indicada, devengará intereses desde el traslado de la demanda hasta el efectivo pago. La tasa será la activa vencida en que en descuentos a treinta días aplica el Banco de la Nación Argentina (Conf. esta Cámara, Sala II, plenario de hecho en la causa 6.378/92 del 08/08/95).

VII. Por último y según lo dispuesto por el art. 34, última parte, de la ley de marcas corresponde confirmar la orden dispuesta por el a quo respecto de publicar la parte dispositiva de esta sentencia por un día y a costa de la demandada en el diario La Nación.

VIII. Voto porque se modifique la sentencia de primera instancia en los términos de los considerandos V y VI, con costas…

El doctor Gustavo R. Recondo dijo:

I. Adhiero y comparto la solución propuesta por mi colega doctora Graciela Medina en su voto en cuanto modificó la sentencia de primera instancia en los términos de los Considerandos V y VI con costas a la vencida.

II. Sin perjuicio de lo cual me permito una aclaración.

Lo que aquí se discute es si la utilización por parte de la demandada de las marcas de la actora como palabra clave "keyword" en el sistema de enlaces patrocinados de los distintos buscadores de internet constituye una infracción marcaria. Sobre este punto, comparto la opinión de mi colega en el sentido de que estando acreditado que ambas partes son competidoras no cabe duda que la accionada se ha aprovechado indebidamente del prestigio ajeno para posicionarse en el mercado, incurriendo así en una infracción marcaria y en un acto de competencia desleal. Para resolver de este modo, observo que no debe influir en la decisión del presente la invocación que efectuó la demandada en su expresión de agravios respecto del carácter notorio del signo ORGANIZACIÓN VERAZ ya

que —como expresé— ambos participan del mismo mercado.

Al respecto cabe remitir a las consideraciones emitidas por mí al fallar en la causa "MD Distribuciones SA c/ Quick Foods SA s/ cese de oposición al registro de marca" del 17-9-02. Allí señale que las características que debe reunir una marca para ser notoria se refieren a: a) el grado de capacidad distintiva que tenga, ya sea por ser inherente al signo o ya sea por adquisición; b) la extensión geográfica del área comercial en la que la marca es usada; c) como consecuencia de "a" el grado de reconocimiento que tenga la marca notoria en el área comercial en la que está compitiendo con la marca joven o en todo el mercado. Este último ítem, torna importante la diferenciación que alguna doctrina y legislación efectúan entre marca notoria y marca de gran renombre: En el primer caso, la dilución puede producirse en el universo de un determinado tipo de comprador, pero no en otro, como por ejemplo si se tratare de la caracterización de un producto sólo adquirido por la gran industria pero no por el consumidor medio. En este caso, la protección —siempre excepcional y por tanto de aplicación restringida en materia de marcas notorias— debe efectuarse respecto del mercado en donde la dilución puede producirse. Por lo contrario, si se tratare de una marca de gran renombre (es decir, conocida aún en los sectores en donde el producto muy improbablemente vaya a ser adquirido: Rolex y Ferrari) la dilución podrá producirse también en los lugares en los que la competencia comercial no exista. Es por este último motivo, que también discrepo en la categorización de Dassas en punto a que si la casi totalidad de los compradores potenciales a los que una marca esta destinada, conocen esta marca, se puede hablar de notoria; porque, salvo, si se aplicare la doble categoría a la que me vengo refiriendo, quedarían afuera las marcas de renombre que, estimo, deben ser protegidas aún con mayor razón que las que limitan su fama casi exclusivamente al sector de los eventuales compradores del producto.

Con respecto a la indemnización de daños y perjuicios comparto la solución propuesta por mi colega doctora Graciela Medina en su voto.

Por ello voto porque se modifique la sentencia apelada en los términos de los considerandos V y VI del voto de la doctora Graciela Medina, con costas de ambas instancias a la vencida.

Graciela Medina. Ricardo Gustavo Recondo.

Caso Kosten *versus* Mercadolibre

VOCES

Mercado virtual. Responsabilidad civil. Derecho comparado. Defensa del consumidor. Negligencia del consumidor. Falta de responsabilidad

Cámara Nacional de Apelaciones en lo Comercial SALA D

En Buenos Aires, a 22 de marzo de 2018, se reúnen los Señores Jueces de la Sala D de la Excelentísima Cámara Nacional de Apelaciones en lo Comercial de la Capital Federal, con el autorizante, para dictar sentencia en la causa "KOSTEN, ESTEBAN C/ MERCADO LIBRE S.R.L. S/ ORDINARIO"…

A la cuestión propuesta, el Señor Juez de Cámara, doctor Heredia dijo:

1º) El señor Esteban Kosten promovió la presente demanda contra Mercado Libre S.R.L. para lograr el resarcimiento de los daños y perjuicios que derivaron de la falta de entrega de un automotor que dijo haber adquirido en el sitio web de ventas y subastas que organiza y administra dicha sociedad. Al respecto, afirmó haber pagado el precio de compra mediante giros internacionales con intervención de una empresa local (modalidad que, según sus dichos, le habría indicado la demandada), así como una suma para cubrir "gastos de entrega y documentación" de acuerdo al pedido que al efecto le hizo Mercado Libre S.R.L., pero que pese a todo ello nunca recibió el rodado. Reclamó, en concreto, se condene a la demandada al pago de cuanto abonó por la frustrada operación, a la reparación del daño moral y para que se le aplique una multa en concepto de daño punitivo. Encuadró el reclamo en normas de la ley de defensa del consumidor y del Código Civil entonces vigente (fs. 45/47 y 65).

Mercado Libre S.R.L. resistió la pretensión del actor oponiendo una excepción de falta de legitimación pasiva como defensa de fondo, que fundó en los siguientes sustanciales argumentos: I) explicó que la plataforma de ventas y subastas on line que explota se divide en dos secciones, una destinada a la compraventa de bienes no registrables, en la que los datos del vendedor son dados a conocer al adquirente sólo después de que este decide concretar la operación haciendo "click" en el botón "comprar" (sección de "marketplace"), y otra vinculada a la adquisición de bienes registrables, con relación a la cual los datos personales del vendedor están publicados en la misma oferta, funcionando en tal caso la plata-

forma como una simple sección de avisos ("sección de clasificados") que permite a los interesados contactarse directamente, sin necesidad de tener que manifestar previamente una voluntad de compra ni registrarse en el sistema; II) sostuvo que la operación a la que se refiere la demanda se canalizó en el marco de la segunda sección y que, por tanto, el actor y la vendedora del automotor se vincularon "… de manera independiente y por fuera de la mencionada plataforma comercial…"; III) adujo que su posición neutral con relación a las operaciones concretadas en la plataforma es advertida a los usuarios en los "Términos y Condiciones" que necesariamente deben ser leídos y aceptados al momento de registrarse como tales; IV) refirió que el servicio de "Mercado de Pago" que administra conjuntamente con la plataforma electrónica no se aplica en la "sección clasificados" sino solamente en la referente a bienes no registrables (sección "marketplace"), y que ni siquiera el relato del actor vinculado a cómo abonó el precio del automotor se condice con el funcionamiento del mencionado canal de pagos (fs. 121 vta./122).

En subsidio de la reseñada excepción, Mercado Libre S.R.L. contestó demanda, pidiendo su rechazo, por las siguientes razones: I) el actor se contactó con un supuesto vendedor quien lo estafó con artilugios que quedaron reflejados en los mails intercambiados por ambos, haciéndose incluso pasar como representante de Mercado Libre S.R.L.; II) la maniobra ilícita se consolidó, además, por la propia negligencia, ligereza o imprudencia del actor, quien no hizo caso de la sospecha que naturalmente generaba la defectuosa redacción que tenían los mails que recibía del supuesto vendedor y del llamativo bajo precio del automotor ofertado (menor de la mitad de su valor en plaza), así como que procedió a trasferir los fondos para pagarlo sin conocer a la persona destinataria y sin previamente constatar la condición física y jurídica del rodado; III) no hubo ningún cobro de comisión por venta por parte del sitio web y que el pago que el actor dijo haber hecho para cubrir "gastos de entrega y documentación" no fue tal sino que se relacionó con el pago de la publicación del aviso en la "sección de clasificados", a lo cual también fue inducido por el supuesto vendedor; IV) no puede ser considerada una responsable solidaria en los términos del art. 40 de la ley 24.240 y, a todo evento, debe el actor demostrar la negligencia o culpa del operador electrónico, ya que no se trata de un supuesto de responsabilidad objetiva; V) el supuesto vendedor que estafó o defraudó al actor debe considerarse un tercero por el que no debe responder Mercado Libre S.R.L.; y VI) los resarcimientos reclamados son improcedentes e inconstitucional la

multa por daño punitivo pretendida (fs. 129/147 vta.).

2º) La sentencia de primera instancia admitió la excepción de falta de legitimación pasiva opuesta por Mercado Libre S.R.L. y rechazó la demanda…

3º) El actor plantea agravios que, en sustancia, pretenden que las cuestiones implicadas se resuelvan a base de una aplicación genérica de principios o reglas vinculadas a cuáles son los derechos del consumidor y las obligaciones del proveedor, la asimetría entre ambos, la omisión informativa en la que había incurrido la demandada y el valor que la confianza tiene en el comercio electrónico, entre otros, sin reparar en que la problemática que plantea el sub lite es bastante más compleja que ello.

Para poner el caso en su justo quicio, es imperioso advertir, ante todo, que el vigente derecho argentino no ofrece un plexo normativo especial relacionado con la responsabilidad de los prestadores de mercados electrónicos como el que organiza y explota la demandada para la venta y/o subasta "on line" de bienes.

Consiguientemente, la visión del derecho comparado sobre ese particular ámbito se presenta como necesaria pues, ciertamente, ofrece ella una guía lo suficientemente razonable como para fijar los estándares jurídicos aptos para resolver con equidad y justicia.

No me anima en la adopción de ese camino ningún desvío extranjerizante, sino la convicción de que el derecho comparado puede servir para fundar decisiones justas, basadas en criterios que han recibido aceptación en países con un desarrollo jurídico similar al nuestro. Como lo ha expresado Enrique Martínez Paz, "… la razón del fecundo aporte que el derecho extranjero lleva a la doctrina y al derecho nacional se muestra evidente y clara si se considera que todas las naciones cuya cultura tiene un común origen, desarrollan las mismas instituciones y puede aquel que las ha llevado a un desenvolvimiento más pleno en su texto o en su aplicación, servir de inspiración para los otros derechos. La vida jurídica de todos los pueblos acreditaría la realidad de este modo de utilización del derecho comparado. La doctrina jurídica nacional es constantemente influida por los movimientos jurídicos que se agitan en el extranjero, y una vez la doctrina elaborada, influye poderosamente en la jurisprudencia, en la aplicación de la ley. De modo, pues, que ni los jueces ni los expositores de materias jurídicas dejan de citar, de apoyar sus conclusiones, en cuanto se trata de casos extraordinarios, en las constancias del derecho comparado; pocos habrían ya que se atrevieran a

pensar que la ley es una fuente mágica de la que el ingenio pueda extraer todas las soluciones…" (conf. Martínez Paz, E., Introducción el Derecho Civil Comparado, Buenos Aires, 1960, ps. 73/74…).

4º) En la materia de que tratan estas actuaciones representa un hito de insoslayable mención la Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8/6/2000, relativa a "Determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior", cuyo contenido normativo ha sido incorporado por los países de la Unión Europea a sus derechos internos con análogos alcances (Alemania: "Telemediengesetz" o TMG de 26/2/2007; Inglaterra: "Electronic Commerce —EC Directive— Regulations" de 2002; Francia: ley 2004-575 de 21/6/2004; Italia decreto-legislativo nº 70/2003; España: ley 34/2002 de 11 de junio; Austria, ley 152/2001; Bélgica, ley de 11/3/2003; Dinamarca: ley 227/2002; Finlandia: ley 459/2002; Francia: leyes 719/200 y 575/2004; Grecia: decreto 131/2003; Islandia: ley 30/2002; Noruega; ley 35/2003; Portugal: decreto 7/2004; Suecia: ley de 6/6/2002; Holanda: ley del 13/5/2005; etc.).

En cuanto aquí interesa, la Directiva 2003/31/CE fijó reglas relacionadas con la "Responsabilidad de los prestadores de servicios intermediarios" (Sección 4), entre las que destacan las siguientes:

"… Artículo 14. Alojamiento de datos

1. Los Estados miembros garantizarán que, cuando se preste un servicio de la sociedad de la información consistente en almacenar datos facilitados por el destinatario del servicio, el prestador de servicios no pueda ser considerado responsable de los datos almacenados a petición del destinatario, a condición de que:

a) el prestador de servicios no tenga conocimiento efectivo de que la actividad a la información es ilícita y, en lo que se refiere a una acción por daños y perjuicios, no tenga conocimiento de hechos o circunstancias por los que la actividad o la información revele su carácter ilícito, o de que,

b) en cuanto tenga conocimiento de estos puntos, el prestador de servicios actúe con prontitud para retirar los datos o hacer que el acceso a ellos sea imposible…".

"… Artículo 15. Inexistencia de obligación general de supervisión

1. Los Estados miembros no impondrán a los prestadores de servicios una obligación general de supervisar los datos que transmitan o almacenen, ni una obligación general de realizar búsquedas activas de

hechos o circunstancias que indiquen actividades ilícitas, respecto de los servicios contemplados en los artículos 12, 13 y 14.

2. Los Estados miembros podrán establecer obligaciones tendientes a que los prestadores de servicios de la sociedad de la información comuniquen con prontitud a las autoridades públicas competentes los presuntos datos ilícitos o las actividades ilícitas llevadas a cabo por destinatarios de su servicio o la obligación de comunicar a las autoridades competentes, a solicitud de éstas, información que les permita identificar a los destinatarios de su servicio con los que hayan celebrado acuerdos de almacenamiento…".

El Tribunal de Justicia de la Comunidad Europea ha resuelto que las precedentes disposiciones se aplican, entre otros casos, a los prestadores de servicio en Internet que facilitan el contacto entre vendedores y compradores de productos, pues la Directiva 2000/31/CE, tal como indica su título, se refiere a los "servicios de la sociedad de la información, en particular el comercio electrónico", quedando por ende comprendidos los servicios prestados a distancia a través de equipos electrónicos de tratamiento y almacenamiento de datos, a petición individual de un destinatario de servicios y, normalmente, a cambio de una remuneración, resultando evidente que la explotación de un mercado electrónico reúne todos esos elementos (conf. TJCE, 12/7/2011, "L'Oréal S.A., Lancôme parfums et beauté & Cie SNC, Laboratoire Garnier & Cie, L'Oréal (UK) Ltd. c/ eBay International AG", apartado 109. El citado fallo del TICE fue dictado como respuesta al requerimiento de explicación prejudicial efectuado el 22/5/2009 por la High Court of Justice [England and Wales], Chancery Division).

De otro lado, el mismo tribunal comunitario europeo ha destacado que los referidos preceptos de la Directiva 2000/31/CE pretenden restringir los casos en los que, conforme al Derecho nacional aplicable en la materia, puede generarse la responsabilidad de los prestadores de servicios intermediarios de la sociedad de la información (conf. TJCE, 23/3/2010, "Google France y Google", apartado 107).

Así pues, el espíritu y la finalidad del régimen aprobado por los transcriptos arts. 14 y 15 se caracteriza por definir una zona libre de responsabilidad a favor de los proveedores de servicios de intermediación en la sociedad de la información que los coloque al amparo de la inseguridad jurídica que se deriva de la posible aplicación de otros regímenes de responsabilidad (conf. Cavanillas Mugica, Santiago, Responsabilidades de los proveedores de información en Internet, Editorial Comares, Granada, 2007, p. 158).

Esa zona libre de responsabilidad alcanza a la materia civil, penal o administrativa (conf. Peguera Poch, Miguel, La exclusión de responsabilidad de los intermediarios en internet, Editorial Comares, Granada, 2007, p. 322).

Ahora bien, como claramente lo expuso el Tribunal de Justicia de la Comunidad Europea en uno de los casos ya citados ("L'Oréal S.A."), la circunstancia de que el servicio prestado por el operador de un mercado electrónico comprenda el almacenamiento de información que le facilitan sus clientes vendedores no basta por sí misma para concluir que, en cualquier caso, a tal servicio le es aplicable lo dispuesto en el artículo 14, apartado 1, de la Directiva 2000/31/CE, pues esa disposición debe interpretarse no sólo teniendo en cuenta su tenor sino también su contexto y los objetivos perseguidos por la normativa de la que forme parte (apartado 111). A ese respecto, para que el prestador de un servicio en Internet quede comprendido en el ámbito de aplicación del artículo 14 de la Directiva 2000/31/CE, es esencial que sea un "prestador intermediario" en el sentido que el legislador ha querido dar a esta expresión en la sección 4 del capítulo II de esta Directiva (apartado 112). Y no es tal el caso cuando el prestador del servicio, en lugar de limitarse a una prestación neutra de dicho servicio mediante un tratamiento meramente técnico y automático de los datos facilitados por sus clientes, desempeña un papel activo que le permite adquirir conocimiento o control de tales datos (apartado 113). De tal suerte, el mero hecho de que el operador de un mercado electrónico almacene en su servidor ofertas de venta, determine las condiciones de su servicio, sea remunerado por el mismo y dé información general a sus clientes no puede implicar que se le excluya de las exenciones de responsabilidad previstas por la Directiva 2000/31/CE (apartado 115). Pero cuanto, por el contrario, este operador presta una asistencia consistente, entre otras cosas, en optimizar la presentación de las ofertas de venta en cuestión o en promover tales ofertas, cabe considerar que no ha ocupado una posición neutra entre el cliente vendedor correspondiente y los potenciales compradores, sino que ha desempeñado un papel activo que le permite adquirir conocimiento o control de los datos relativos a esas ofertas. De este modo y por lo que se refiere a esos datos, tal operador no puede acogerse a la excepción en materia de responsabilidad prevista por el artículo 14 de la Directiva 2000/31/CE (apartado 116). En ese marco, corresponde al órgano jurisdiccional analizar si el operador del mercado electrónico ha desempeñado o no el papel descrito precedentemente en relación con las ofertas de venta (apartado 117). Así, en el supuesto de que el órgano jurisdiccional llegue a la conclusión de que el operador no ha teni-

do un comportamiento limitado a una posición neutra entre el cliente y el vendedor, sino que ha desempeñado un papel activo, corresponderá a los tribunales indagar si, en las circunstancias que concurren en el litigio, el operador del mercado electrónico ha cumplido los requisitos exigidos por el artículo 14, apartado 1, letras a) y b), de la Directiva 2000/31/CE para poder acogerse a la excepción en materia de responsabilidad (apartado 119). En efecto, en el supuesto de que este prestador se haya limitado a un tratamiento meramente técnico y automático de los datos y, en consecuencia, le sea aplicable lo dispuesto en el artículo 14, apartado 1, de la Directiva 2000/31/CE, tal operador sólo podrá, no obstante, quedar exento de cualquier responsabilidad en virtud de dicho apartado 1 respecto de los datos de carácter ilícito que ha almacenado cuando no haya tenido "conocimiento efectivo de que la actividad o la información es ilícita" y, en lo que se refiere a una acción por daños y perjuicios, no haya tenido "conocimiento de hechos o circunstancias por los que la actividad o la información revele su carácter ilícito", o cuando, tras haber adquirido conocimiento de estos extremos, haya actuado con prontitud para retirar los datos en cuestión o hacer que el acceso a ellos sea imposible (apartado 119). Es decir, corresponde al órgano jurisdiccional analizar si el operador del mercado electrónico ha tenido, en relación con las ofertas de venta en cuestión, conocimiento de hechos o circunstancias por los que la actividad o la información revele su carácter ilícito. A este último respecto, para que se le niegue a dicho operador la exención de responsabilidad prevista por el artículo 14 de la Directiva 2000/31/CE, basta con que haya tenido conocimiento de hechos o circunstancias a partir de los cuales un operador económico diligente hubiera debido deducir ese carácter ilícito y actuar de conformidad con lo establecido en el apartado 1, letra b), de dicho artículo 14 (apartado 120). La cuestión indicada debe interpretarse en el sentido de que se contempla cualquier situación en la que el prestatario en cuestión adquiera conocimiento, de una forma o de otra, de tales hechos o circunstancias (apartado 121). Así pues, encajan en este supuesto, en particular, tanto la hipótesis de que el operador de un mercado electrónico descubra la existencia de una actividad o información ilícitas como consecuencia de una investigación realizada por su propia iniciativa como la hipótesis de que le sea notificada la existencia de este tipo de actividad o información. En el segundo caso, si bien es cierto que el hecho de que se realice una notificación no determina automáticamente que el operador pierda la posibilidad de invocar la exención de responsabilidad, puesto que la notificación de la existencia de actividades o informaciones supuestamente ilícitas puede resultar excesivamente imprecisa

o no encontrarse suficientemente fundamentada, no es menos cierto que tal notificación constituye, como regla general, un elemento que el juez debe tomar en consideración para apreciar, habida cuenta de la información que se ha comunicado de este modo al operador, si éste tenía realmente conocimiento de hechos o circunstancias a partir de los cuales un operador económico diligente hubiera debido constatar ese carácter ilícito (apartado 122).

Es de observar que en el mismo sentido que el Tribunal de Justicia de la Comunidad Europea que se acaba de reseñar, cuya doctrina ha sido divulgada en nuestro medio por la doctrina especializada (conf. Palazzi, P., La responsabilidad civil del mercado virtual por oferta de productos en infracción al derecho de marcas: el caso "L'Oréal v. eBay", ED 244-52), se orientó la jurisprudencia de EE.UU al igualmente declarar que el operador del mercado electrónico de ventas o subastas on line no tiene el deber de aventar infracciones sin un conocimiento específico de ellas (sentencia dictada en el caso "Tyffany Inc. c/ eBay Inc.", 576 F. Supp., 2d. 463, 469 S.D.N.Y. 2008, caso relacionado con la venta de joyería falsificada en el sitio web de la parte demandada).

Asimismo, es la orientación adoptada en Bélgica (conf. Bruxelles, Tribunal de Commerce, 7ème Chambre, Salle B, 31/7/2008, "Lancôme Parfums et Beauté & Cie c/ eBay International AG, eBay Europe s.a.r.l., et s.p.r.l. eBay Belgium"), y en época más reciente por la Casación Francesa en una sentencia (conf. Cour de Cassation, Chambre commerciale, financière et économique, 3/5/2012, "eBay c/ Louis Vuitton Malletier"), que, a la vez, implicó desautorizar expresiones anteriores de la jurisprudencia francesa que, por el contrario, responsabilizaban a los operadores por ilícitos perpetrados a través del mercado electrónico bajo el argumento de ser empresas de corretaje que no están exentas de garantizar que su sitio web no se utilice con fines reprensibles ya que asumen dos roles diferentes como host de web y editor de servicio.(conf. Tribunal de Grande Instance de Troyes, Chambre Civile, 4/6/2008, "Hermès International c/ Madame Cindy F., S.A. eBay France et eBay International"; Tribunal de Commerce de Paris 1er., Chambre B, 30/6/2008, "Louis Vuitton Malletier c/ eBay Inc., eBay International AG". Para un comentario sobre este último precedente, véase: Marín López, J., Responsabilidad civil de sitios de subastas por infracciones marcarias, en la obra coordinada por Palazzi, P., "La responsabilidad Civil de los intermediarios en Internet", Buenos Aires, 2012, p. 393 y ss.).

De tal suerte, teniendo en cuenta la normativa y la jurisprudencia reseñada hasta

aquí (la última normalmente vinculada a casos de infracciones marcarias pero con conceptos trasladables mutatis mutandi a otras situaciones en las que se pone en tela de juicio la responsabilidad de los operadores de mercados virtuales), así como a otras expresiones del derecho comparado que ofrecen respuesta a aspectos distintos pero afines a los reseñados, el régimen jurídico que juzgo aplicable en su proyección al derecho nacional es el siguiente:

a) Puede hablarse de una exención de responsabilidad del operador de un mercado electrónico de ventas o subastas on line cuando no ha desempeñado un papel activo que le permita adquirir conocimiento o control de los datos almacenados, es decir, cuando ha sido un "mero canal" limitándose a proporcionar un foro para una transacción entre un comprador y un vendedor.

Tal general exención se funda en la circunstancia de que no es posible responsabilizar al operador cuando actúa efectivamente como un mero intermediario, es decir, adoptando entre los destinatarios del servicio (comprador y vendedor) una posición neutra, meramente técnica, automática y pasiva, lo que impide que tenga conocimiento y control de la información almacenada.

Ello, asimismo, es el correlato lógico de que no puede imponerse a los prestadores de servicios de mero almacenamiento (hosting) una obligación general de supervisar los datos que transmitan o almacenen, ni una obligación general de realizar búsquedas activas de hechos o circunstancias que indiquen actividades ilícitas. Esto es así pues se está en presencia de un intermediario que se presenta como un alojador que no tiene obligaciones "proactivas" (conf. Lorenzetti, R., Comercio Electrónico, Buenos Aires, 2001, ps. 278 y 293; Anteproyecto de ley de comercio electrónico argentino, elaborado por la Jefatura de Gabinete del P.E.N., año 2000, art. 38).

De ahí que, a la inexistencia de una obligación general de vigilar le siga, como regla, la inexistencia de responsabilidad, tal como lo declaró nuestra Corte Suprema de Justicia de la Nación al analizar el régimen de responsabilidad de los "motores de búsqueda" en Internet (conf. CSJN, 28/10/2014, "Rodríguez, María Belén c/ Google Inc.s/ daños y perjuicios", considerando 16).

Todo lo anterior es consistente, además, con el hecho de que el acceso al mercado electrónico está estructurado como servicio cuyo contenido prestacional se realiza mediante el desempeño diligente del programa prestacional mismo, sin que el operador del mercado asegure el resultado de los negocios que se pueden celebrar por medio del mismo.

A este orden de cosas responde, precisamente, un precedente de esta alzada mercantil (conf. CNCom. Sala B, 7/3/2017, "Gómez Maciel, Francisco José c/ Dridco S.A. s/ ordinario", caso referente a la adquisición de un automotor en la página web "demotores.com").

b) No obstante, aun si el operador del mercado electrónico hubiera desempeñado una posición neutra, podría ser responsabilizado mediante una condena de daños y perjuicios, no pudiéndose acoger a la exención antes referida, si ha tenido conocimiento de hechos o circunstancias a partir de los cuales un operador económico diligente hubiera debido constatar el carácter ilícito de las ofertas de venta en cuestión y, en caso de adquirir tal conocimiento, no haya actuado con prontitud.

Es que, como lo resolvió el Tribunal Federal de Justicia de Alemania, si bien no puede imponerse al prestador la obligación de controlar la información almacenada antes de que se produzca el acto ilícito (situación ex ante), lo cierto es que una vez que un derecho ha sido violado, el proveedor del alojamiento queda obligado a poner fin a la infracción cuando tenga conocimiento de dicho contenido ilícito, vgr. retirando de manera inmediata la oferta de que se trate, como así también a adoptar las medidas necesarias para impedir que se cometan nuevas infracciones (situación ex post), e indemnizar daños si fuera ello pertinente (conf. BGH, 11/3/2004, "Internetversteigerung I", I ZR 304/01, CR 2004, caso referido a la empresa de subastas on line "Ricardo" en el que se declaró su responsabilidad frente a la empresa fabricante del reloj Rolex; véase también: Martínez, A. y Porcelli, A., Alcances de la responsabilidad civil de los proveedores de Servicios de Internet (ISP) y de los proveedores de servicios on line (OSP) a nivel internacional, regional y nacional – Las disposiciones de puerto seguro, notificación y deshabilitación, Rev. Pensar en Derecho, 2015, nº 6, año nº 4, p. 117, espec. p. 134).

La adquisición del efectivo conocimiento del ilícito tiene lugar a partir de hechos o circunstancias aptos para posibilitar, aunque mediante o por inferencias lógicas al alcance de cualquiera, una efectiva aprehensión de la realidad que se trate (conf. Tribunal Supremo España, sentencia nº 144/2013, del 4/3/2013, "Don Bartolomé c/ Google Inc. y Don Gines", y sus citas de los precedentes del 9/12/ 2009, RC n.º 914/2006 y 10/2/2011, RC n.º 1953/2008).

No obstante, deben quedar a salvo los casos de "ignorancia premeditada" y de "indiferencia imprudente". Si el operador tiene motivos que le hagan sospechar que los usuarios de sus servicios están

cometiendo ilícitos, no le está permitido "apartar la vista" a fin de sustraerse de la responsabilidad. Dicho de otro modo, la "ignorancia premeditada" o la "ignorancia culpable" equivale a un conocimiento efectivo (sentencia dictada en el caso "Tiffany (NJ) INC. y Tiffany y Company v. EBay, Inc.", 600 F.3d. 93 [2010]).

En esta segunda hipótesis que se examina, la responsabilidad del proveedor tiene base subjetiva y se vería comprometida, entre nosotros, de acuerdo al art. 1109 del Código Civil y/o arts. 1716 y 1717 del Código Civil y Comercial de la Nación (doctrina de la CSJN, 28/10/2014, "Rodríguez,María Belén c/ Google Inc.s/ daños y perjuicios", considerando 17; CSJN, 12/9/2017, "Gimbutas, Carolina V. c/ Google Inc. s/ daños y perjuicios", considerando 3º).

Se trata, valga aclararlo, de una responsabilidad no por el contenido ilícito de los datos alojados en el servidor o por las conductas de los usuarios del servicio, sino por el hecho de una omisión o inadecuada, incompleta o injustificadamente tardía retirada de los contenidos o de adoptar la acción necesaria para bloquear el acceso a ellos.

c) En fin, ninguna exención de responsabilidad puede aprobarse cuando el operador del mercado electrónico prestó un papel activo que le permitió adquirir conocimiento o control de los datos almacenados.

Tampoco si ha recibido una orden judicial que lo colocaba en situación de ejercer una "vigilancia activa" o prestó una asistencia consistente, en particular, en optimizar la presentación de las ofertas de venta en cuestión o en promover tales ofertas, vgr. a través de motores de búsqueda externos como Google o Yahoo. Es con este alcance que nuestra jurisprudencia ha aplicado la doctrina sentada en el recordado precedente "L'Oreal" fallado por el Tribunal de Justicia de la Comunidad Europea (véase: CNFed. Civ. Com., Sala I, 5/5/2015, "Nike International Ltd. c/ DeRemate. com de Argentina S.A.", voto de la doctora Najurieta; CNFed. Civ. Com. Sala III, 21/5/2015, "Nike International LTD c/ Compañía de Medios Digitales CMD S.A.", voto de la doctora Medina, en ED del 27/8/2015, con nota de Schotz, G., Responsabilidad de los portales de ventas por infracciones marcarias).

Asimismo, la ausencia de una intermediación pasiva de la información y consiguiente pérdida de la exención de responsabilidad surge cuando el autor del contenido ilícito ha actuado bajo la dirección o control del operador del mercado electrónico (conf. Peguera Poch, Miguel, ob. cit., p. 340).

Y si en estos distintos y particulares casos quedara involucrado un consumidor, la prueba de la participación activa del operador de mercado electrónico (presupuesto fáctico sine qua non) podría generar su responsabilidad en los términos del art. 40 de la ley 24.240 por el riesgo que deriva de tan especial configuración del servicio. Mas si por el contrario está ausente ese específico escenario fáctico, lo dispuesto por el art. 40 de la ley 24.240 no podría recibir aplicación sobre la base de consideraciones generales o abstractas que prescindan de una adecuada indagación acerca de si el operador del mercado electrónico prestó efectivamente un papel activo en los términos indicados. Con lo que va dicho, que sólo con tal limitado alcance correspondería admitir, según lo creo, la responsabilidad "objetiva" por daños propia del derecho del consumo a la que se hace referencia, negando que ello sea posible de un modo más amplio y general contrariamente a lo sostenido por alguna jurisprudencia administrativa y judicial (conf. Dirección General de Defensa y Protección de los Consumidores y Usuarios de la Provincia del Chubut, dictamen del 17/8/2010, Exp. Adm. nº 1275/2008 "S.T.R. R., D. A. c/ Mercado Libre.Com. Ar y/o quien resulte Responsable s/ Denuncia Ley de Defensa del Consumidor"; CNCiv. Sala K, 5/10/2012, "Claps Enrique Martín y otro c/ Mercado Libre S.A. s/ daños y perjuicios"; Cám. 4ª, Civ. Com. Córdoba, 29/12/2016, "Mercado Libre S.R.L. c/ Dirección de Defensa del Consumidor y Lealtad Comercial") y por cierto sector de la doctrina (conf. Fernández, C., La responsabilidad por daños a la luz de la ley de defensa del consumidor en las contrataciones a través de medios informáticos – La resolución condenatoria aplicada por la Dirección de Defensa del Consumidor a Mercado Libre, Revista Argentina de Derecho Comercial y de los Negocios, IJ-LXIV-585; Vignola, M., Compraventa por internet – Comentario al fallo "Claps", Revista Jurídica de Daños, nº 8, marzo 2014, IJ LXXI-48).

d) Se desprende de todo lo expuesto hasta aquí que la manera y el grado en que un operador interactúa con los vendedores y los propietarios es un aspecto fundamental para los tribunales a la hora de determinar la responsabilidad o no del sitio web de mercado electrónico.

En esta materia, como en tantas otras, las generalizaciones son contrarias a un adecuado servicio de justicia.

e) Como regla, el prestador que organiza o gestiona el mercado electrónico no realiza una función de corredor, es decir, no se obliga ante una parte a mediar en la negociación y conclusión de uno o varios negocios, ya que no recibe ningún encargo a ese fin. El núcleo de su prestación,

por el contrario, consiste en un servicio electrónico que permite acceder al conjunto de una información enderezada a la consecución de una finalidad, cual es que unos adquieran productos o servicios que otros enajenan, obteniendo el operador por ese servicio una retribución.

f) Además de los servicios de alojamiento de datos, una plataforma de mercado electrónico como la de Mercado Libre S.R.L. puede ofrecer actividades auxiliares o conexas.

Dichas actividades pueden incluir medios de evaluación o calificación, seguro, modalidades de pago, verificación de la identidad (a menudo realizada por terceros prestadores) o la plataforma puede incluso prestar el servicio subyacente que se ofrece a los usuarios. Bien entendido, la exención de responsabilidad mencionada más arriba se limita a la prestación de servicios de alojamiento de datos y no es extensible a otros servicios o actividades efectuados por la plataforma. Asimismo, dicha exención de responsabilidad tampoco excluye la responsabilidad de la plataforma derivada de la legislación de protección de datos personales aplicable, en la medida en que estén afectadas las propias actividades de la plataforma. En cambio, el simple hecho de que una plataforma realice también otras actividades —además de prestar servicios de alojamiento—, no significa necesariamente que dicha plataforma ya no puede invocar la exención de responsabilidad con respecto a los servicios de alojamiento. En cualquier caso, la manera en que las plataformas diseñan su servicio y aplican medidas voluntarias para hacer frente a los contenidos ilícitos en línea sigue siendo en principio una decisión empresarial y la cuestión de si se benefician de la exención de responsabilidad de los intermediarios debe evaluarse caso por caso (conf. Comisión Europea de la UE, Bruselas, 2/6/2016, "Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones: Una agenda europea para la economía colaborativa", capítulo 2.2 "Regímenes de responsabilidad").

En el contexto precedentemente expuesto, de no admisibilidad de exención de responsabilidad alguna si se trata de daños derivados del incumplimiento de actividades auxiliares o conexas, debe ser ubicado, por ejemplo, lo atinente al sistema "Mercado de Pago" de que se vale la demandada (en este sentido: Cám. Civ. Com. Jujuy, Sala III, 15/9/2016, expte. nº C-031.375/14, "Acción emergente de la ley del consumidor: Ferreiro, Pablo Alberto c/ Mercado Libre S.R.L."; Garzino, M., Contratación electrónica y responsabilidad de los intermediarios - Comentario al fallo Ferreiro, Pablo A. c/

Mercado Libre SRL, Revista de Derecho del Consumidor, nº 2, mayo 2017, IJ CCCXLIV-392).

5º) Descripto in genere el régimen jurídico atinente a los operadores de mercados de compraventas o subastas de bienes on line, cabe ahora observar que el resultado de la prueba rendida en autos demuestra, sin asomo de dudas, que la demandada Mercado Libre S.A. se comportó con relación a la oferta de venta del automotor que interesó al actor como un simple sitio web de alojamiento de datos (hosting).

Al respecto, confirmó el peritaje informático que, en efecto, en el sitio web de la demandada no es necesario registrarse previamente, ni ingresar con usuario o clave, para navegar en la sección avisos clasificados de automotores y que la información relacionada con nombre y teléfono del vendedor es de libre acceso (fs. 350/351, punto 5). Asimismo, el peritaje aportó la captura de pantalla correspondiente a la operación enjuiciada en autos de cuya lectura se desprende que el aviso clasificado respectivo portaba, después de describir el automotor, el nombre y teléfono de la parte vendedora (fs. 351, punto 6), lo cual es compatible con el régimen contractual referente a la publicación de bienes o servicios que se da a conocer a los interesados en una posible adquisición (fs. 301, cláusula 4.2, y fs. 348).

Obviamente, nada de lo anterior es compatible con la idea de que la demandada hubiera desempeñado en el caso un papel activo que le permitió adquirir conocimiento o control de los datos almacenados y publicitados. Antes bien, los indicados aspectos del peritaje evidencian que la demandada se limitó a proporcionar nada más que un foro para una transacción entre un comprador y un vendedor, habiendo simplemente dado un tratamiento meramente técnico y automático de los datos facilitados al efecto.

A todo evento, la exención de responsabilidad favorable a la demandada que deriva de esta última constatación, se ve confirmada además por otros datos distintos pero a la vez de innegable trascendencia que ratifican la inexistencia de un papel activo asumido por la demandada, a saber:

a) En el sitio web de Mercado Libre S.R.L. es fácilmente accesible para cualquier usuario la lectura de los "Términos y Condiciones" del servicio prestado (conf. peritaje informático, fs. 348).

En esos "Términos y Condiciones" se aclara que "… Mercado Libre sólo pone a disposición de los Usuarios un espacio virtual que les permite ponerse en comunicación mediante internet para encontrar una forma de vender o comprar

servicios o bienes…" y que "… Debido a que Mercado Libre no tiene ninguna participación durante todo el tiempo en que el artículo se publica para la venta, ni en la posterior negociación y perfeccionamiento del contrato definitivo entre las partes, no será responsable por el efectivo cumplimiento de las obligaciones asumidas por los Usuarios en el perfeccionamiento de la operación…" (fs. 304).

Estas aclaraciones, puestas a disposición de los usuarios para su lectura de un modo sencillo, cumplen adecuadamente, a mi juicio, con los estándares de información cierta, clara y detallada del servicio que se provee, por lo que no hay incumplimiento de la obligación de información debida a los consumidores en cuanto a la comprensión de los riesgos derivados de su empleo (art. 1107 del Código Civil y Comercial de la Nación; art. 4, primer párrafo, de la ley 24.240; Alterini, J., Código Civil y Comercial Comentado – Tratado Exegético, Buenos Aires, 2015, t. V, ps. 880/881).

b) No hay prueba de que Mercado Libre S.R.L. con anterioridad a la fecha de la operación indicada por el actor hubiera tenido conocimiento efectivo de una ilicitud en ciernes relacionada con el aviso que publicitaba el automotor, como tampoco de hechos o circunstancias que hubieran debido despertar una sospecha suya.

Tampoco fue alegado explícitamente por el actor que la demandada hubiera incurrido en una "ignorancia premeditada" o "ignorancia culpable".

c) No se acreditó en la causa que el actor hubiera tenido acceso al aviso clasificado publicado en el sitio web de la demandada a través de motores de búsqueda en Internet, esto es, merced a un servicio "key words" o enlace privilegiado revelador de una actividad de la demandada enderezada a optimizar la presentación de la oferta.

d) Informó el peritaje informático que el usuario que aparecía como vendedor fue inhabilitado el 10/10/2013 (fs. 356, punto 18), esto es, en una fecha anterior a la indicada en la demanda como de inicio de la compra (15/10/2013; fs. 45) y no se ha acreditado por ninguna otra prueba que el aviso clasificado respectivo hubiera permanecido en el sitio web con posterioridad a tal inhabilitación.

Esta dicotomía de fechas tampoco ha sido explicada por el actor.

e) Es de observar, asimismo, que con relación específica a las operaciones que nazcan de la utilización de la "sección clasificados" (cuya diferenciación con la "sección marketplace" es nítida y no ha sido negada por el demandante), se advierte a los usuarios del sitio web de Mercado

Libre S.R.L., precedido de la frase "… Es bueno saberlo, para estar más atentos…", que "… Nunca recibirás un e-mail de Mercado de Pago por tu compra en Clasificados de Mercado Libre…" (conf. peritaje informático, fs. 335).

Sin embargo, el señor Kosten hizo caso omiso de esto último pues mantuvo reiterados contactos por mail con una cuenta de correo de "Mercado de Pago" que no pertenecía a la demandada (fs. 341, 345 y 357/358), en vez de denunciar la presencia de un "spoof" —mail de un falso remitente— para lo cual la página web de Mercado Libre S.R.L. habilita una específica opción (fs. 355).

Por otra parte, no ha sido probado que la plataforma administrada por la demandada hubiera facilitado o hubiera sido usada para transmitir esos mails apócrificos en condiciones que aquella pudo evitar mediante la utilización de filtros informáticos apropiados u otras tecnologías de identificación o investigación (sobre este aspecto y su impacto en el régimen de responsabilidad de los proveedores de servicios, véase: Almark, D. y Molina Quiroga, E., *Tratado de Derecho Informático*, Buenos Aires, 2012, t. III, p. 16 y ss.).

f) Más allá de la negligencia del actor en la producción de la prueba informativa dirigida a Arper Express S.R.L. (fs. 394), lo cierto es que, según sus propios dichos, el pago internacional del precio se realizó con intervención de esta última empresa (fs. 45), esto es, no se hizo a través del sistema "Mercado de Pago" que ofrece la demandada.

Consiguientemente, debe descartarse cualquier responsabilidad de la demandada derivada de la utilización del tal servicio auxiliar o conexo de acreditación de pagos. Ello es así, máxime ponderando que tampoco está probado lo dicho por el actor en el sentido de haber sido la demandada quien le sugirió la utilización del indicado canal de pago internacional.

g) Mercado Libre S.R.L. no cobró comisión alguna por la operación referida en estas actuaciones (conf. peritaje contable, fs. 362 y vta.).

h) La especial hipótesis admitida más arriba de eventual aplicación del art. 40 de la ley 24.240 no se da en absoluto en la especie, y no sirve para concluir lo contrario las generalidades en las que incurre la expresión de agravios del actor cuando apela a la idea del consumidor como parte débil, a su asimetría frente al proveedor, a la dificultad probatoria del caso, etc.

6º) Lo expuesto y concluido en el considerando anterior es ya suficiente para propiciar la confirmación del fallo de la

instancia anterior en cuanto rechazó la demanda.

Sin embargo, no puede ser silenciado, a modo de consideración obiter dictum, que el actor ha sido víctima de su propia torpeza (art. 1111 del Código Civil y art. 1729 del Código Civil y Comercial de la Nación).

En efecto, sabido es que los recaudos que ha de adoptar el adquirente de un automotor son esencialmente dos: verificación física del vehículo y verificación de su situación jurídica. La última (verificación jurídica) aparece impuesta por el artículo 16, decreto 6582/58 ("A los efectos de la buena fe prevista en los artículos 2, 3 y 4 del presente, se presume que los que adquieren derechos sobre un automotor conocen las constancias de su inscripción y de las demás anotaciones que respecto de aquél obran el Registro de la Propiedad del Automotor, aun cuando no hayan exigido del titular o del disponente del bien la exhibición del certificado de dominio que se establece en este artículo"), de cuyos términos surge que a ese fin es necesario contar con el certificado que hace referencia la disposición citada. Si ese certificado no ha sido solicitado, el adquirente no podrá invocar buena fe, porque el error derivará de su propia negligencia que, naturalmente, no podrá ser alegada para justificarse. En cuanto a la verificación física, ella es impuesta por el art. 6 del decreto 335/88, y quien no la llevara a cabo como previa a la adquisición tampoco podría ser considerado adquirente de buena fe (…).

Pues bien, no surge de las constancias de la causa, ni el actor siquiera lo ha alegado, que hubiera procedido a cumplimentar las apuntadas verificaciones jurídica y física antes de proceder a pagar el precio mediante una transferencia de fondos a quien, por otra parte, llamativamente se presentaba ante él como una persona residente en país extranjero (fs. 12).

Y todo ello lo hizo, además, sin que al parecer le llamase la atención que el precio que se le exigía era notoriamente menor al de mercado de un vehículo como el que pretendió adquirir (véase informe de fs. 264).

En tales condiciones, corresponde recordar que nadie puede alegar su propia torpeza para sacar provecho de ella: nemo audire debet turpitudem propiam allegans (conf. CSJN, Fallos 301:48; esta Sala D, 19/9/07, "Angelini, Fernando Gabriel c/ Banco de la Provincia de Buenos Aires s/ ordinario").

…

8º) Por lo expuesto … propongo al acuerdo confirmar la decisión de primera instancia,

con excepción de lo atinente a las costas del juicio, las que en ambas instancias deben correr en el orden causado…

Concluida la deliberación los señores Jueces de Cámara acuerdan:

(a) Confirmar la decisión de primera instancia, con excepción de lo atinente a las costas del juicio, las que en ambas instancias deben correr en el orden causado.

Reseña de libros

RESEÑA DE LIBROS

por Jorge J. Vega Iracelay

Legal Tech. La transformación digital de la abogacía
Director: Moisés Barrio Andrés
Edición: junio de 2019, 648 pp.
ISBN: 978-84-9020-851-9
ISBN Digital: 978-84-9020-852-6

It has become appallingly obvious that
our technology has exceeded our humanity.
Albert Einstein

Este libro publicado por la Editorial Wolters Kluwer España, en su primera edición, está dirigido por Moisés Barrio Andrés, experto y referente en Derecho Digital y de las TIC, y fundador de una nueva rama del Derecho, el Derecho de los Robots o *Robot Law*, y cuenta con la colaboración como coautores de destacados expertos en los temas allí tratados. La obra expone de manera práctica pero acabada los principales aspectos en los que la aplicación de la transformación digital y sus herramientas conocidas bajo el genérico de Legal Tech están afectando a la abogacía y al resto de las profesiones jurídicas, coadyuvando a su transformación. La disrupción de estos nuevos desarrollos tecnológicos se manifiesta de manera exponencial por su rapidez y dimensión, revolucionando la industria legal tradicional. Sin embargo, como suele suceder en estas disrupciones tecnológicas, además de las oportunidades que nos ofrecen, ellas no están ausentes de desafíos. En tal sentido, esta obra describe ambos efectos con un acertado equilibrio facilitando al lector la formación de su propia opinión de manera informada. No hay área en los servicios jurídicos que no se vea impactada por esta disrupción tecnológica, sea aquella el ejercicio de la abogacía por cuenta propia, como miembro de un despacho o asesoría jurídica, o para el resto de las profesiones jurídicas, como por ejemplo los servicios de la

Justicia. Este libro tiene el acierto de analizar todas ellas, así como otros desarrollos tecnológicos de vanguardia que también representan dicha disrupción, como *blockchain*, inteligencia artificial, *fintech* o *smart contracts* y sus implicaciones prácticas para los profesionales jurídicos como sus usuarios.

En la obra, cuya reseña ofrecemos de manera apretada, se analizan asimismo distintos ecosistemas en la adopción y uso de servicios Legal Tech, como el español, el de los Estados Unidos de América, Reino Unido, y el mexicano —en el que tuvimos el honor de colaborar con nuestra autoría—, dándonos una visión detallada y práctica sobre la oferta de soluciones y aplicaciones Legal Tech, su madurez en dichos mercados, y sus oportunidades y desafíos. De una manera holística pero novedosa, la obra analiza asimismo el impacto de los servicios Legal Tech en la investigación, el empleo, la formación jurídica y en las funciones registrales y notariales. No menos importante es el análisis del impacto del uso de la tecnología en la rentabilidad de las firmas legales. Finalmente, nada cambiará sino cambiamos la manera de razonar el Derecho, con esquemas mentales y prismas más propios de las ciencias de la computación, tratados en esta obra en el capítulo sobre Legal Thinking.

En el marco de un clima de zozobra y cierto desconocimiento por el impacto de la digitalización en nuestros trabajos, funciones, destrezas y modelos de negocios, por citar algunos, esta obra se presenta como un faro que arroja luz sobre ellos y nos orienta a un desembarco seguro. La aceitada y estratégicas visión y coordinación de su director, el profesor y abogado Moisés Barrio Andrés, añade un valor extraordinario a los exhaustivos y versados análisis de cada capítulo. Su lectura es ágil, con un lenguaje jurídico asequible para cualquier lector, cautivante y de interés, y de un entramado sólido en su contenido.

Sus capítulos nos ofrecen información y herramientas prácticas para enfrentar de manera eficaz y ágil la disrupción de la Legal Tech, y coadyuvar así en la transformación profunda de nuestra profesión, catalizada por la disrupción tecnológica. Sin lugar a dudas, esta obra representa un parteaguas en la producción académica sobre la materia de la Legal Tech en idioma español, contribuyendo con su investigación y análisis al progreso de la Ciencia Jurídica en este campo.

Este libro es una lectura obligada para los profesionales jurídicos cualquiera sea el ámbito de su desempeño, administradores de despachos y asesorías jurídicas, estudiantes de derecho, autoridades y docentes de las universidades de derecho, profesionales de recursos humanos, así como para los desarrolladores de herramientas digitales enfocadas a la industria legal, y para todo aquel que quiera tener un entendimiento acabado de su metamorfosis actual.

No menos importante: esta obra es un llamado de atención para las facultades de Derecho para transformar la manera en que enseñamos el Derecho, así como para los profesionales de recursos humanos en el área legal en la contratación, desarrollo y retención de talento.

En las propias palabras de Moisés Barrio Andrés en el prólogo de este libro: "Esperamos con estas páginas crear una imagen poliédrica del cambio que ya está en marcha en las profesiones jurídicas, así como brindar claves prácticas para afrontar con éxito la transformación digital y la implantación de aquellas herramientas de la Legal Tech que nos ayuden a ser más eficientes. Con estos cambios estaremos a la altura del resto de los sectores que ya han evolucionado".

Pero quizás lo más importante de esta obra sea su llamado a cambiar nuestros arquetipos mentales, y enfrentar el presente y el futuro con pragmatismo, estrategia y anticipando el cambio, capitalizando las oportunidades que la tecnología nos ofrece para acometer con éxito la transformación que nuestra profesión requiere en este siglo XXI. De esta manera, complementaremos nuestro criterio jurídico, pensamiento estratégico, empatía y emociones como abogados-personas, con la automatización de tareas y tratamiento exhaustivo de datos que nos ofrece la Legal Tech, convirtiendo nuestro trabajo en uno de naturaleza más intelectual y de mayor valor añadido. Este libro se nos ofrece como una ruta del éxito en ese camino.

Quizás al decir de Einstein nos veamos excedidos en nuestra humanidad por la tecnología, pero estamos ante una oportunidad histórica de capitalizar sus ventajas y enfrentar con inteligencia sus desafíos, centrándola en nuestra única y preciada humanidad.

Autores

Gonzalo Bleda

Jurista del Centro de Arbitraje y Mediación de la Organización Mundial de la Propiedad Intelectual (OMPI). Licenciado en Derecho por la Universidad Pontificia de Comillas (ICADE, Madrid, España) cuenta con un máster en asesoría jurídica empresarial por el Instituto de Empresa (IE Law School, Madrid, España) y un máster especializado en Derecho de la Propiedad Intelectual por Queen Mary, University of London (Reino Unido). Antes de incorporarse a la OMPI, fue asociado en el departamento de Derecho Mercantil de Garrigues y enfocó su especialización en Derecho de la Propiedad Intelectual y de las Tecnologías. Con anterioridad trabajó en el departamento de Derecho Mercantil de PwC enfocado en empresas del sector de la tecnología.

Guillermo Cabanellas

Licenciado en Economía (1971) y abogado (1972) por la Universidad Nacional de Buenos Aires. Máster en Derecho Comparado (1975) y doctor en Ciencias Jurídicas (1978), University of Illinois (Estados Unidos). Socio del Estudio Cabanellas, Etchebarne, Kelly Abogados. Profesor de posgrado de la Facultad de Derecho de la Universidad de Buenos Aires. Profesor de posgrado de la Universidad Austral Argentina. Profesor de Derecho de la Universidad de San Andrés. Autor de más de cien artículos de Derecho y Economía publicados en Argentina, Alemania, España, Estados Unidos, Reino Unido, Japón y Polonia. Autor de más de treinta libros de Derecho y Economía publicados en Argentina, Alemania, Estados Unidos y Países Bajos.

Andrés Chomczyk

Es abogado (Universidad Austral), con estudios de posgrado sobre Derecho Tecnológico y protección de datos (Universidad Católica Argentina, Universidad de San Andrés y Universidad de Santiago de Compostela). Es investigador invitado del CETyS de la Universidad de San Andrés y actualmente se desempeña como asesor legal independiente para varias compañías y organizaciones de la industria blockchain.

Rodolfo Christophersen

Abogado recibido en la Universidad de Buenos Aires. Posgrado en Asesoramiento Jurídico de Empresas (UBA). Profesor invitado en la Carrera de Especialización de Derecho Informático de la UBA, en la Diplomatura en Derecho 4.0 de la Universidad Austral y en la Maestría en Derecho Empresario de la Universidad del ESEADE. Especialista en temas de Derecho y Tecnología, Innovación Legal y Responsabilidad de los Intermediarios. Gerente Corporativo de Legales y Relaciones Gubernamentales del área de Resolución de Disputas de Mercado Libre.

Ignacio de Castro

Director de la división de Controversias en materia de propiedad intelectual y relaciones exteriores del Centro de Arbitraje y Mediación de la Organización Mundial de la Propiedad Intelectual (OMPI) en Ginebra, Suiza. Es abogado español y también ha obtenido el título de "solicitor" en Inglaterra. Posee un máster por el King's College de Londres. Antes de incorporarse a la OMPI en 2002, ejerció la abogacía en Baker & McKenzie y en Freshfields Bruckhaus Deringer, Londres, en las esferas del arbitraje y litigios internacionales. Nació en España.

Carla Delle Donne

Máster en Crimen Internacional y Justicia, Universidad de Torino – UNICRI; especialista en Derecho Penal, Universidad del Salvador; secretaria en la Procuraduría de Crímenes Económicos y Lavado de Activos.

Julián Dunayevich

Licenciado en Ciencias de la Computación, egresado de la Facultad de Ciencias Exactas y Naturales (Universidad de Buenos Aires). Actual director de NIC Argentina, una de las instituciones que dieron origen a Blockchain Federal Argentina (BFA). Fue uno de los pioneros en lo que respecta a las primeras conexiones en Internet en Argentina y contribuyó al desarrollo de la red en toda la región.

Daniela Dupuy

Fiscal de Primera Instancia en lo Penal, Contravencional y de Faltas, y actualmente fiscal a cargo del Equipo Especializado en Delitos Informáticos de la Ciudad Autónoma de Buenos Aires. Doctora en Derecho Penal y Procesal de la Facultad de Derecho de la Universidad de Sevilla, España. Máster en Leyes, Universidad de Palermo. Posgrado sobre Ciberdelincuencia en la Universidad Internacional de Cataluña, España. Directora de los libros *Cibercrimen I* y *Cibercrimen II*, Editorial B de F, Argentina-Madrid, 2016.

Daniel Franca

Licenciado en Ciencias de la Comunicación Social (Universidad de Buenos Aires). Integra el equipo de Comunicación de NIC Argentina y Blockchain Federal Argentina (BFA). Especialista en Comunicación de la Tecnología. Ha liderado proyectos en el portal educ.ar y el Ministerio de Educación, y ha participado como productor periodístico en la TV Pública Argentina y otros medios.

Leonor Guini

Abogada de la Universidad de Buenos Aires (UBA). Obtuvo su título de posgrado como abogada especialista en Derecho de la Alta Tecnología en la Universidad Católica (2005). Ha desarrollado proyectos de regulación compleja en seguridad. También ha participado como asesora legal en proyectos tecnológicos relacionados con temas de firma electrónica/digital, protección de datos, historia clínica digital y en temas afines a la propiedad intelectual. Se encuentra certificada por la Asociación Española de Calidad como delegada en Protección de Datos, cargo que desempeña actualmente en Gire S. A. como DPO Externa. Es adjunta del posgrado de Derecho Informático de la UBA y consultora en temas relacionados con el Derecho de las Nuevas Tecnologías de la Información.

Mariana Kiefer

Máster en Leyes, Columbia University, especialista en Derecho Penal, Universidad Torcuato Di Tella. Docente de la Universidad de Buenos Aires. Es secretaria de Primera Instancia, Fiscalía Especializada en Delitos Informáticos N.º 12 de la Ciudad Autónoma de Buenos Aires.

Lucía Suyai Mendiberri

Abogada, graduada en la Universidad de San Andrés, donde también cursó el Programa de Derecho y Tecnología de las Comunicaciones. Asociada del estudio Bruchou, Fernandez Madero & Lombardi en el Departamento de Propiedad Intelectual, Privacidad y Nuevas Tecnologías. Además, es investigadora del Centro de Tecnología y Sociedad de la Universidad de San Andrés, en el que integra el IA LAB.

Pablo A. Palazzi

Abogado. Máster en Leyes, International Trade Law de Fordham Law School. Socio del estudio Allende & Brea. Co-director del Centro de Tecnología y Sociedad de la Universidad de San Andrés. Director y fundador de la *Revista Derecho y Nuevas Tecnologías* y de la *Revista Latinoamericana de Protección de Datos Personales*. Es autor de los libros: *Delitos contra la intimidad informática*" (2019), *Delitos informáticos* (2015), *Informes comerciales* (2007), *La protección de los datos personales en la Argentina* (2005) y *Transferencia internacional de datos personales* (2000).

Javier Alejandro Papaño

Abogado. Agente de la propiedad industrial, especialista en Derechos Intelectuales y profesor de derechos reales e intelectuales (Universidad del Museo Social Argentino y Universidad Católica de Santiago del Estero, Departamento Académico Buenos Aires).

Ariel E. Provenzani Casares

Abogado (Universidad de Buenos Aires). Asesor y representante legal interno y externo de diversas empresas públicas y privadas. Profesor y expositor sobre distintas cuestiones de derecho procesal y fintech en la Universidad Nacional de Lomas de Zamora, UBA, Colegio de Abogados de Morón y Universidad del Este. Autor de distintos artículos sobre la especialidad. Integrante de la Mesa de Innovación del Banco Central.

Gabriela Ramírez

Licenciada en Ciencia Política de la Universidad de Buenos Aires. Desde 2016 se desempeña como subdirectora nacional de NIC Argentina, liderando la visión estratégica y la gestión operativa de la institución. Actualmente forma parte de Blockchain Federal Argentina y coordina el Grupo de Trabajo de Políticas de LACTLD, la asociación que agrupa a todos los Country Code Top Level Domain. En especial, promueve el trabajo local y regional en torno a la gobernanza de Internet.

Leandro Toscano

Es jefe de la Unidad de Desarrollo de Operaciones del Centro de Arbitraje y Mediación de la Organización Mundial de la Propiedad Intelectual (OMPI) en Ginebra, Suiza. Es abogado de la Universidad de Buenos Aires. Obtuvo una maestría en la Universidad de Londres (Queen Mary University of London y University College London) en solución internacional de controversias, y posee una especialización en Derecho de la Alta Tecnología en la Pontificia Universidad Católica Argentina. Antes de incorporarse a la OMPI, en 2008, trabajó como abogado en las áreas de propiedad intelectual y tecnologías de la información. Fue el representante del Centro de la OMPI en su oficina situada en Singapur desde el año 2011 hasta mediados del año 2014.

Camila Trentadue

Licenciada en Ciencias de la Comunicación Social de la Universidad de Buenos Aires, con orientación en publicidad y opinión pública. Actualmente se desempeña como jefa de Comunicación en NIC Argentina, desde donde participa en diversas iniciativas vinculadas a la gobernanza de Internet. Participa en Blockchain Federal Argentina y es parte del equipo organizador del Youth IGF Argentina, el foro de discusión del país que busca ampliar las voces de los y las jóvenes en las discusiones de gobernanza de Internet. A su vez, dicta talleres sobre Comunicación, Medios y Cultura en YMCA.

Jorge J. Vega Iracelay

Es profesor e investigador de Tecnología y Sociedad en la Universidad Panamericana, Infotec y *Nexos*. Es director sénior de Asuntos Jurídicos, Corporativos y RSE - Microsoft, México.

Tamara Zylbersztejn

Es estudiante de la carrera de Ciencias de la Comunicación de la Universidad de Buenos Aires e integra el equipo de Comunicación de NIC Argentina. Apasionada por la comunicación y el periodismo, se ha desempeñado como coordinadora del área de comunicación y prensa de la Fundación INECO organizando y gestionando actividades académicas y de concientización en conjunto y en simultáneo con instituciones como la Fundación Favaloro, la Fundación River Plate, la Academia Estadounidense de las Artes y las Ciencias, la Universidad de Cambridge y la Universidad Diego Portales. A su vez, dictó talleres de radio y producción radial en Radio Arinfo. Hoy en día, desde NIC Argentina, participa de diferentes proyectos tecnológicos.

El segundo número de la *Revista Derecho y Nuevas Tecnologías* se terminó de imprimir en el mes de febrero de 2020, en los talleres de Docuprint, Ciudad Autónoma de Buenos Aires, Argentina.

RDYNT
Número 2

Revista Derecho y Nuevas Tecnologías

ISSN 1514-1918
9 771514 191003 >