Derecho y Tecnología

EL SUPLEMENTO LEGAL DE NEURONA BA

MAYO 2021
ED: Nº04

Con el objetivo de acompañar el debate acerca de la expansión en el uso de las tic y su impacto en el derecho, desde Neurona BA lanzamos este suplemento sobre *"DERECHO Y TECNOLOGÍA".* Tiene la coordinación de nuestro columnista habitual, el abogado, docente e investigador, Ernesto Liceda, con una amplia trayectoria en estas temáticas.

AUTORES

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

ARIEL VERCELLI // Abogado, Escribano, Doctor en Ciencias Humanas y Sociales, Investigador de CONICET, Instituto de Humanidades y Ciencias Sociales(INHUS – CONICET / UNMdP).

JOSE FRANCISCO ARCE // Abogado, Especialista en Derecho de Internet. Presidente de la ONG Desarrollo Digital.

ISMAEL LOFEUDO // Abogado, Especializado en Derecho Informático y Nuevas Tecnologías. Docente del Seminario de Derecho Informático Facultad de Ciencias Jurídicas y Sociales (UNLP). Miembro del Grupo de Investigación en Tecnologías de Información Facultad de Ciencias Económicas (UNLP)

BÁRBARA VIRGINIA PEÑALOZA // Abogada (Facultad de Derecho de la UNCuyo). Máster en Abogacía Digital y Nuevas Tecnologías(Universidad de Salamanca). Vicepresidente 2da de Asociación Derecho Informático Argentina (ADIAR).

PRÓLOGO

Por Ernesto Liceda

Es un lugar común plantear que el derecho llega tarde, que tal situación no está regulada o, más recientemente, que el derecho no tiene que "bloquear" el desarrollo económico. Ante este contexto es preciso realizar algunas consideraciones. En primer lugar, estas críticas sólo se centran en el derecho positivo, es decir en aquellas regulaciones plasmadas en leyes, decretos y otros instrumentos, **no en el derecho en su totalidad.**

Mal podría pensarse que el derecho, en tanto conjunto de normas sociales, creado y modificado por la sociedad puede llegar tarde a dicha sociedad. Los usos y costumbres, por ejemplo, son derecho así como los principios que pueden o no estar plasmados en un instrumento legal sancionado por la autoridad competente.

Que aquellos que deben dar resolución a los conflictos ante ellos presentados den vuelta la cara a esta realidad no es óbice a que ella exista. La máxima del derecho civil y comercial de que los jueces no pueden dejar de dictar sentencia so pretexto de oscuridad o falta de resolución en la ley positiva no hace más que reconocer que el derecho es más que el código civil y comercial.

Entiendo que es preciso detenernos particularmente en la afirmación de que "el derecho no debe bloquear el desarrollo", es una forma más amigable de decir que el Estado no debe meterse con el mercado. Un fallo de tierras lejanas (o no tanto) pudiera ser uno de los primeros ejemplos de la necesidad de emprender este camino. *"Si un modelo de negocio determinado no garantiza el cumplimiento de las regulaciones de la UE, este modelo de negocio debe cambiarse. No es el modelo de negocio el que determina la validez de las normas de la UE, sino las normas de la UE que determinan la permisibilidad de un modelo de negocio"* **(Foodwatch c. Amazon, Tribunal del Distrito de Múnich).**

Es preciso destacar que la normativa afectada es el reglamento 543/2011 de la UE, dictado en protección de los consumidores. Y esto es lo que, entiendo, debemos tener siempre en cuenta. Cuando algunos secto-

res plantean que determinada norma impide el desarrollo de tal o cual producto o modelo, tal vez sea porque tal producto o modelo no sea valioso para la sociedad. Incluso más, podemos encontrar muchos ejemplos de "desarrollos" que directamente violentan la normativa vigente sin ningún tipo de sanción. En la violación sistemática de la dignidad de las personas tenemos múltiples ejemplos de modelos de negocios no muy virtuosos que desconocen absolutamente tanto la ley de protección de datos como el código civil y comercial.

Lamentablemente la inacción de los organismos del Estado genera lo que se conoce como *evasión institucionalizada".* En otras palabras, todos sabemos que dicha acción está prohibida, pero sabemos también que nadie nos va a sancionar. De mantenerse esta situación en el tiempo podríamos llegar a lo que los abogados conocemos como desuetudo, es decir, la derogación de una norma por la costumbre.

Entrando ya en la presentación de los artículos que componen el presente suplemento, el lector encontrará un trabajo muy interesante y clarificador de **Ariel Vercelli** titulado "***Tecnologías blockchain, tokens no-fungibles y escasez artificial"***, donde el autor no sólo explica en forma clara y concisa de qué hablamos cuando hablamos de blockchain, sino que lo complementa con los NFT, interpelando al lector sobre el camino que va tomando el sistema económico mundial. Podríamos traer a colación la venta de la imagen de la "niña desastre" que fue vendida por u$s 500.000 precisamente, como un NFT.

Por otra parte, **José F. Arce** nos presenta, desde Córdoba, su trabajo titulado ***"Violencia de género ejercida por medios digitales"*** un trabajo que, entiendo, debería ser leído por todas las personas que ejerzan la docencia en estos tiempos de educación virtual. Ello puesto que se trata de un artículo donde se brindan definiciones sumamente claras y se explican diferentes casos específicos de violencia de género en entornos digitales.

Por último, tenemos dos trabajos que, a mi modo de ver, deberían ser leídos en estéreo. Por un lado el de **Ismael Lofeudo** (que juega de local puesto que es de La Plata) titulado "***Ciberestafas la otra epidemia"***; y por el otro, el de **Bárbara Virginia Peñaloza** quien, desde Mendoza, nos presenta su trabajo ***"Ciberfraudes en pandemia: Defendiendo al consumidor".*** Estos dos artículos son de imprescindible lectura para todo aquel que tenga una cuenta en el banco. La solvencia de ambos autores al momento de abordar el tema desde perspectivas diferentes, pero claramente complementarias demuestran la necesidad de abordar los problemas (particularmente los delitos) en la sociedad red en forma transdisciplinaria.

Aunque los cuatro trabajos parecen abordar temas sumamente diferentes, hay un vocablo que los une y sobre el que invito al lector a reflexionar. La identidad.

Espero que los artículos resulten de utilidad e interés para todos.

TECNOLOGÍAS BLOCKCHAIN, TOKENS NO-FUNGIBLES Y ESCASEZ ARTIFICIAL

ARIEL VERCELLI
Abogado, Escribano, Doctor en Ciencias Humanas y Sociales,
Investigador de CONICET,
Instituto de Humanidades y Ciencias Sociales
(INHUS – CONICET / UNMdP).

El inicio del siglo XXI está marcado por la invención de la tecnología *blockchain* (en español cadena de bloques) y su vínculo indisoluble con la criptomoneda "Bitcoin". La idea de una *blockchain* fue presentada en 2008 por Satoshi Nakamoto (un seudónimo, tal vez una persona física o un grupo de ellas). La blockchain puede definirse como una tecnología de registro distribuido (en inglés, *distributed ledger technology*) que permite estructurar y administrar registros compartidos, en línea y en constante crecimiento. Se las puede definir como un libro contable (una base de datos, un tipo de archivo) que, mediante el uso intensivo de criptografía (cálculos, matemática), tiene la capacidad de mantener de forma permanente e inalterable (según configuraciones), el registro cronológico de todos los intercambios que han tenido lugar (transacciones) dentro de una red. Las blockchain permiten crear historias de los datos. Muchas de estas redes funcionan a través de protocolos par a par (P2P) y sus registros pueden ser abiertos y distribuidos. De allí que estas redes tiendan a funcionar con protocolos de consenso entre múltiples personas, entidades y/o nodos.

Cada uno de ellos mantiene una copia completa e idéntica de ese libro de transacciones. Por ello, estas redes se caracterizan por ser un modelo de gestión transparente aunque de escritura limitada. Es decir, todos pueden analizar el registro, mirarlo, copiarlo, pero sólo algunos pueden escribir en él. Para escribir es necesario tener la capacidad de hacerlo (capacidad computacional / criptográfica, cumplir ciertos requisitos o, también, ser miembro de una red privada / cerrada). Las blockchain se estructuran a través de bloques que se agregan cronológicamente (se suman) a una cadena. Cada bloque contiene la información transable, responde a un tiempo y lugar y está unido (matemática y criptográficamente) a la cadena a través de funciones hash (un proceso matemático de una sola vía). Si alguno de los bloques es suprimido o alterado, entonces, toda la cadena de bloques se corrompe (pierde su continuidad). Dependiendo de las configuraciones de las redes, aquellos que procesan y confirman la información obtienen pequeñas ganancias o incentivos (económicos, simbólicos, de prestigio, etc.). Por lo general, se usan computadoras especialmente diseñadas y de gran procesamiento de cálculo para resolver los problemas criptográficos.

Las blockchain se pueden clasificar de acuerdo a sus niveles de participación, apertura o acceso: existen redes público-comunitarias (distribuidas y abiertas), redes con permisos de acceso (permisionadas, con admisión) o redes blockchain privadas (cerradas). Las blockchain públicas se han convertido en herramientas poderosas para el diseño y construcción de entornos de confianza: logran prescindir de intermediarios, terceros de confianza o autoridades externas a la misma red. Estas redes se están proyectando para garantizar la integridad y fiabilidad de intercambios: comercio, sistema financiero / fintech, políticas públicas en salud (COVID19 e historias clínicas), Internet de las cosas, registros de la propiedad (muebles e inmueble), gestión del valor intelec-

tual (registros de obras, patentes, marcas), seguros, trazabilidad de activos, gestión de archivos y documentación.

Una de las iniciativas más innovadoras sobre blockchain es Ethereum (descrita en 2013 por Vitalik Buterin). En Ethereum se utiliza la criptomoneda Ether como incentivo para los que ofrecen el "poder computacional" o su "participación" para sostener la red. Las blockchain de segunda generación como Ethereum permiten desarrollos innovadores sobre todo tipo de servicios: entre otros, aplicaciones distribuidas (dapps), organizaciones autónomas descentralizadas (DAOs) o la creación y uso de tokens. Ethereum se caracteriza por haber implementado los "smart contracts / contratos inteligentes" (a partir de ideas de Nick Zabo en 1984). Se trata de piezas de código con términos preestablecidos y que se ejecutan a través de la misma red. Los "contratos inteligentes" (diferentes de los contratos jurídicos) usan los tokens para registrar e identificar quiénes son las partes involucradas (personas físicas, jurídicas, virtuales).

Dentro de las blockchain los token tienen multiplicidad y diversidad de usos. Pueden usarse para representar activos digitales o bienes materiales. Incluso, pueden asociarse tanto a activos fungibles (por ejemplo, un bitcoin que puede intercambiarse uno por otro) como a activos no-fungibles (por ejemplo, un avatar dentro de un mundo virtual). Específicamente, estos últimos, los tokens no-fungibles o NFT (por sus siglas en inglés, non-fungible tokens), fueron diseñados para que no resulten mutuamente intercambiables. Los NFT pueden definirse como piezas de información digital que, gracias a la criptografía y el uso blockchain, resultan únicas y distinguibles. De allí que, por definición y diseño, los NFT se caractericen por ser únicos (no hay dos iguales); indivisibles (no se pueden fraccionar); inagotables (mientras perdure su blockchain); complejos de falsificar; y, sobre todo, transferibles a otros titulares (de aquí su potencialidad para los negocios).

La caracterización de los NFT permite ahora avanzar sobre un punto clave. Los NFT tienen la capacidad de asociar / transportar algunas de sus características a cualquiera de los bienes a los que se unan (sean bienes digitales, intelectuales o materiales). Estos bienes pueden tener (o tienen) una existencia completamente independiente y ajena a los NFT que les sirven de contenedor dentro de una blockchain. Ahora bien, sólo cuando a estos bienes o activos se les asocian los NFT, entonces pasan a compartir sus características artificiales de unicidad. Por ello, los NFT bien pueden considerarse un agregado ortopédico, o externo, un contenedor, un envoltorio, una etiqueta que se asocia a estos bienes producidos en los más diversos espacios y tiempos. Los NFT tienen como principal función crear un tipo de escasez artificial (programable, configurable) y que bajo ciertas condiciones espacio-temporales pueden transportarse hacia los más diversos bienes.

Los NFT son una de las mejores expresiones en el uso de la blockchain y la criptografía para crear una especie de escasez registrable y coleccionable en los entornos digitales. La unicidad es inmediatamente, y por definición, una escasez relacional. Esta configuración particular de tokens no fungibles permite que ciertos bienes puedan asociarse a la unicidad y, que ello, los transforme en activos coleccionables y negociables. Los coleccionistas e inversores otorgan un valor particular a las piezas únicas que permiten acumular valor y luego ser transferidas. Esta es una idea recurrente: intercambiar bienes a partir de relaciones de "mercado" donde se supone que la escasez (de bienes, productos o servicios) favorece una suerte de puja sobre el precio (valor). Por ello, quienes negocian un NFT están intercambiando algo similar a una criptomoneda pero con un token especial que fue diseñado para crear unicidad y cierto tipo de escasez.

Los NFT no son nuevos, algunas iniciativas ya tienen más de 4 años de existencia dentro de la red Ethereum. Estos tokens comenzaron a atraer la atención de los usuarios y coleccionistas

cuando se introdujo el estándar de los token ERC721. El éxito de los "CryptoKitties" es un claro ejemplo: se trata de un juego dentro de la red Ethereum que permite crear, criar y coleccionar gatos digitales y donde cada gato tiene un código genético único digital gracias al uso de tokens no fungibles. En la actualidad los NFTs comienzan a abarcar las más diversas experiencias humanas y sus usos potenciales son ilimitados. Pueden servir para volver coleccionables todo tipo de bienes: desde obras digitales, performances, jugadas, memes, imágenes, archivos de audio o video, datos, partidas de videojuegos, jugadas deportivas, obras de arte digital, experiencias registradas, tierras dentro de mundos virtuales, identidades / avatares, certificados, identidades, etc.

En 2021 los espacios de intercambio de NFT también comenzaron a ganar mayor volumen y especificidad. La mayoría hacen uso de Ethereum (aunque también hay otras blockchain como Tron, Neo o Eos). Entre otros, se pueden citar OpenSea, Rarible, Sorare, Decentraland, Enjin, CryptoPunks, NBA Top Shots, CryptoUNStamps. Las blockchain (incluyendo los NFT y otros instrumentos en desarrollo) comienzan a percibirse como una gran oportunidad para "las y los artistas" digitales. Incluso, el 24 de marzo de 2021 la Sociedad Italiana de Autores y Editores (SIAE) y la empresa de finanzas Algorand (fundada por el criptógrafo Silvio Micali, MIT, Boston, USA) presentaron un ambicioso proyecto orientado a crear una plataforma abierta basada en cadena de bloques, pública y accesible a cualquier persona, que permita gestionar por diseño (by design) los derechos de autor de sus asociados. Al respecto anunciaron la creación de 4.000.000 millones de NFT para que estén asociados a las obras intelectuales de los más de 95.000 autores inscriptos en la SIAE. Los italianos buscan que su iniciativa escale a la gestión colectiva mundial.

La tecnología blockchain se expande cada día más. Su crecimiento marca la emergencia de nuevas formas de registro, colección e intercambio de valor. Los NFT son una prueba de ello. La creación artificial y programable de escasez en el mundo digital aún parece atraer adeptos. Sus ideas no son nuevas: establecimiento de fronteras, control de accesos, medidas tecnológicas, modelos de negocio basados en la escasez y la promesa de grandes rentabilidades. Es claro, los NFT no llegan solos, también son herederos de una larga tradición. Con su emergencia se reavivan viejas tensiones entre la unicidad y la multiplicidad, entre la abundancia y la escasez, entre los supuestos originales y sus copias, entre los criptógrafos y los descifradores. En momentos en que la copia (la acción de copiar) es vital, abundante, pervasiva, distribuida, omnipresente, es necesario preguntarse: ¿a quiénes beneficia el diseño de escasez artificial en los entornos digitales?

VIOLENCIA DE GÉNERO EJERCIDA POR MEDIOS DIGITALES

JOSÉ FRANCISCO ARCE
Abogado, Especialista en Derecho de Internet.
Presidente de la ONG Desarrollo Digital.

Las manifestaciones de violencia, como una especie de relaciones sociales basada principalmente en el uso de recursos para conseguir algo de otro u otros (a fin de que haga o soporte) encontró en los espacios digitales un campo propicio no solo para expandirse con rapidez y amplificar sus efectos, sino también para perpetuarse en el tiempo, convirtiéndose así internet en un lugar/espacio para los actos constitutivos de violencia de género (VG en adelante).

Definimos a la violencia de género digital (VGD) como una forma de violencia exteriorizada en acciones directas o indirectas, públicas o privadas, cometida a través de nuevas tecnologías, o espacios digitales (conectado o no a internet) que se perpetúa negativamente en persona o un grupo de personas en razón de su género, que daña esencialmente la privacidad, la dignidad y la intimidad humana.

Como figura autónoma, la VGD debería ser una modalidad más a las enunciadas en la Ley 26.485, Artículo 6, y que principalmente está contemplada en la violencia psicológica, por un lado, por las graves consecuencias en la salud de las personas y por otro, en la violencia simbólica debido a la repetición y perpetuación en los medios digitales de mensajes, patrones y valores estereotipados que reproducen dominación o desigualdad.

Entorno Digital ¿Por qué es importante entenderlo?

Sabemos que el entorno digital plantea desafíos, pero rara vez las personas imaginan las consecuencias ni reflexionan sobre sus usos (el uso lo impone el mercado). Son tantos los beneficios y sin aparentes costos, que parece algo implícito su plena bondad. Pero, una mirada atenta, revela que es este quien termina definiendo muchas conductas, sobre todo las de los consumidores irreflexivos. Entonces, por el lado de lo tecnológico, al usar los dispositivos como hasta ahora, terminamos siendo ausentes testigos de una metamorfosis conductual[1]. Y por otro, el de la cultura, ante la ausencia de lo que llamamos un plan de "ciudadanía digital" vemos que los usos y consumos se traducen en materia de VG, en apropiaciones que no son solamente la reproducción de actos o acciones estereotipadas, sino consumos masivos y la percepción de los mismos, muchas veces como algo gracioso. Es primordialmente algo cultural. Por ello, pensar el entorno digital significa un compromiso a ser parte activa, a concientizar ciertas reglas preestablecidas, y pasar de ser consumidor pasivo a prosumidor reflexivo y críticos.

Consolidación de la VG en entornos digitales

Si bien ya hemos mencionado algunas circunstancias que han permitido la digitalización de las manifestaciones de VG, podemos resumir en cuatro (4) aspectos claves que han permitido que el ejercicio de actos de VG se arraigue en los entornos digitales. A saber: *a.- Relación desigual de poder en tecnología b.- La objetivación del cuerpo de las mujeres en Internet c.- La brecha de género digital d.- Anonimato en Internet.*

Clasificación

Existen diversas clasificaciones[2] respecto a las formas en las que se ejerce la violencia contra las mujeres en el ámbito digital. Tomando en cuenta que Twitter se ha convertido en la principal plataforma para promover campañas de odio contra las mujeres, Amnistía Internacional[3] la VGD que ataca directamente las expresiones de las mujeres en plataformas como Twitter, con el objetivo final de silenciarlas, puede consistir en:

- Amenazas directas o indirectas de violencia física o sexual.
- Insultos dirigidos a uno o varios aspectos de la identidad de una mujer, como los de carácter racista o transfóbico.
- Acoso selectivo.
- Atentados contra la intimidad, como el doxeo[4].
- Divulgación de imágenes sexuales o íntimas de una mujer sin su consentimiento.

Consecuencias

Estas formas de violencias causan graves daños psicológicos y emocionales, refuerzan los prejuicios, dañan la reputación y causan pérdidas económicas. Muchas mujeres al ser víctimas, abandonan las redes, se autocensuran, mantienen un bajo perfil o utilizan pseudónimos, afectando su pleno desarrollo y profundizando la brecha de género.

Las víctimas y las supervivientes experimentan depresión, ansiedad y miedo y, en algunos casos, hasta tendencias suicidas. La violencia facilitada por la tecnología también puede dar lugar a daños físicos (incluidos suicidios), así como perjuicios económicos. ... Los perjuicios económicos pueden producirse cuando la imagen de una víctima de abusos cibernéticos aparece en varias páginas de resultados de los buscadores, lo que dificulta a la víctima la obtención de empleo…[5]

Casos Particulares configurativos de VGD

a.- Acoso Digital o CiberBullying: El acoso digital como forma de hostigamiento a las mujeres y niñas puede tomar varias formas e intensidades, pero básicamente pueden ser simplemente actos para molestar, humillar, hacer seguimientos o control de las víctimas[6] hasta acoso sexual. Aquí, dos fallos que ilustran situaciones desde distintos puntos de vista:

La sentencia de Córdoba "D.N. y Otras p.ss.aa de Lesiones Leves"[7] , muestra que no todo tipo de acoso debe ser sometido al fuero penal[8]. En el caso, una menor de edad sufrió acoso de compañeras de colegio durante varios años, con daño psicológico leve. Concluyendo el tribunal sobre estos hechos que: *...resulta más oportuno y apropiado, implementar vías alternativas de resolución de conflictos, lo cual constituye una posibilidad de aprendizaje no sólo para el joven sino también para todo el conjunto social, puesto que no puede ocultarse que la sociedad, conducida por adultos, cuando es violenta, conduce a los niños, niñas y adolescentes en ese mismo derrotero.*

En sentencia del Juzgado de control de 4° Nominación Córdoba[9] en un caso de *upskirting* o fotografiar mujeres por debajo de la pollera, se aplicó perspectiva de género y diversas multas, entre ellas la de someterse a un tratamiento terapéutico.

b.- Difusión de no consentida de material íntimo: Esta situación nace de la práctica conocida como *sexting*. Es decir, el envío y recepción de material digital referido a la intimidad. La difusión de material íntimo no consentidas (mal llamada pornovenganza) que refiere a la distribución o publicación del mismo en redes a fin de humillar y menoscabar la dignidad (en este caso sin coacción ni amenazas) constituye una de las prácticas más difundidas. Situación que, si bien no es un delito autónomo, aunque sí tipificado como tal en el proyecto del CP del 2018[10], se subsume en delitos de acuerdo a las conductas desplegadas[11].

Como se menciona en el trabajo del CELE "La Regulación de la Pornografía no consentida en Argentina"[12] esta situación debe ser abordada

desde la vulneración de derechos fundamentales y como acto que requiere una condena penal.

c.- Discursos de Odio: Si bien la difusión no consentida de material íntimo es considerada como una forma de discurso de odio por incitar a la violencia contra la mujer, existen otras formas como los troll (personajes digitales anónimos o con nombres falsos que injurian y agreden en internet) que se constituyen en una forma de discriminación (reconocido por Belén Do Para y CEDAW).

Estos discursos son comunes en nuestra jurisprudencia[13], a saber: El derecho a una vida libre de violencia, tanto en el ámbito público como en el privado, también incluye el derecho de la mujer a ser libre de toda forma de discriminación. ...las expresiones empleadas en la red social de acceso público Facebook...se muestran altamente injuriantes. Repárese que algunas de las locuciones utilizadas fueron *"...Feminazzi..."; "...Femiyihadista..."; "...Genocida de Hombres..."; "...Centro de detención Clandestino llamado Polo de la Mujer"; "...hombres tengan huevos y enfrenten a las genocidas #ni una menos..."*, *términos que denotan una conducta lesiva y agresiva que lisa y llanamente encuadra en el concepto de violencia simbólica, generando otros tipos de violencia y desigualdad.*

d.- Acoso/Abuso Sexual por medios digitales *(Grooming[14]):* Cuando los ataques son dirigidos contra niñas o adolescentes mujeres menores de 18 años tratando de obtener fotos o videos de su intimidad, estas acciones pueden calificar como acoso o abuso digital en línea, -art. 131 CP-. Se trata de un proceso abusivo, donde el agresor va a intentar ganarse la confianza del NNyA de manera paulatina para luego atacar directamente su sexualidad.

En concreto mencionamos que, aun sin contacto físico, este tipo de accionar constituye un acoso y abuso sexual y así lo ha entendido la Sala Penal del TSJ de Córdoba al dejar claramente establecido que aunque no exista contacto corporal directo o inmediatez física entre la víctima y el agresor, el abuso sexual se configura porque, en palabras de quienes emitieron dicha sentencia: *(...)Abusar sexualmente supone utilizar (indebidamente), el cuerpo de la víctima para actos de significado objetivo impúdico. ... Contacto corporal de índole físico sexual siempre existió, toda vez que las víctimas fueron obligadas a efectuarse tocamientos de significado objetivamente impúdico, pero a instancias del autor y sin contacto de este sobre el cuerpo de las mismas.*[15]

Conclusión

El derecho afronta grandes desafíos a no poder dar respuestas efectivas con las medidas tradicionales debido a que el escenario donde todo ocurre escapa a las jurisdicciones muchas veces y es aquí donde cobra importancia la cooperación pública-privada y, donde el debate actual sobre la moderación de contenido en las grandes plataformas tiene parte de las respuestas que necesitamos.

La violencia digital como manifestación de las distintas formas de violencia ya reconocidas, se configura en un nuevo escenario necesitando ser abordada de forma específica y con perspectiva de género. Así se menciona en el reporte *"Ciber violencia contra las mujeres y niñas: una llamada de atención al mundo"* elaborado por la comisión de Banda Ancha de ONU (2015) que convoca a interpretar la CEDAW "Bajo el lente del siglo 21". [16]

[1] No hacemos nada, muchas veces porque no entendemos lo que está pasando y otras porque no hubo normas claras desde temprana edad, ni parámetros de usos virtuosos desde que comenzamos los tecnofactos.
[2] La organización mexicana Luchadoras que detallan 13 modalidades de VGD. https://luchadoras.mx/nosotras/
[3] Informe de Amnistía Internacional #ToxicTwitter: Violence and Abuse against Women Online.
[4] Anglicismo que refiere a la acción de divulgar en internet de datos privados que revelan la identidad de una persona con el fin de acosarla o causar malestar.
[5] ONU, Informe de la Relatora Especial sobre la violencia contra la mujer, sus causas y consecuencias acerca de la violencia en línea contra las mujeres y las niñas desde la perspectiva de los derechos humanos, A/HRC/38/47, 2018.
[6] Entre las conductas podemos encontrar también las denominadas cyberstalking (acoso o acecho) o doxxing.
[7] La sentencia N 65 del año 2020 de la Cám. Criminal de Villa María. Conductas que podrían ser disparadoras VGD en otras situaciones y que no siempre configuraban delitos.
[8] Al contrario del cód.penal Español que lo tipifica en el art 172 ter.
[9] Causa "Cipolla Sánchez, Mariano Hernán p.s.a. Infracción a la Ley 10.326 (Código de Convivencia Ciudadana" Agravado por ser funcionario público, de fecha: 9 de abril de 2019.
[10] Texto publicado en la revista jurídica digital "Pensamiento Penal", edición del 25/6/18. En la publicación en la página web del Ministerio de Justicia y Derechos Humanos de la Nación hay una referencia sintética dividida por temas. La podemos ver en el apartado de delitos informáticos. accesible en: https://www.argentina.gob.ar/justicia/nuevocodigopenal/temas/delitos-informáticos
[11] Ver fallo de Justicia Federal "Ramirez Carlos Raúl s/ Recurso de casación". CFCP, Sala II, fallo del 6/2/18 (Reg. N 2/18).
[12] Disponible en: https://www.palermo.edu/cele/pdf/Paper-regulacion-pornografia.pdf
[13] Cámara de Familia 2a Nominación. Córdoba, "C., A. -DENUNCIA POR VIOLENCIA DE GÉNERO - RECURSO DE APELACIÓN", 2017.
[14] Habrá notado el lector que se han usado diversos préstamos lingüísticos como Grooming, Sexting, UpSkirting, Stalking denominados anglicismos porque vienen de la lengua Inglesa. . Es dable destacar aquí que al ser tantos se traducen en una penetración cultural peligrosa, por lo cual se recomienda el uso de términos del propio lenguaje.
[15] Sala Penal Tribunal Superior de Justicia, Córdoba, "CARIGNANO, Franco Daniel p.s.a. producción de imágenes pornográficas de menores de 18 años, etc. -Recurso de Casación-", 2020.
[16] Disponible en https://www.unwomen.org/-/media/headquarters/attachments/sections/library/publications/2015/cyber_violence_gender%20report.pdf?v=1&d=20150924T15

CIBERESTAFAS LA OTRA EPIDEMIA

ISMAEL LOFEUDO
Especializado en Derecho Informático y Nuevas Tecnologías.
Docente del Sem. de Derecho Informático Fac.Cs.Jcas y Soc. UNLP.
Miembro del Grupo de Investigación en Tecnologías de Información
Fac. Cs. Econ. UNLP

"Hola Buenas tardes, me presento, mi nombre es Ricardo, asesor de ANSES. Estoy retomando la comunicación de ANSES debido al bono de Ingreso Familiar de Emergencia, tiene conocimiento del bono por favor?..."

Esa frase se repitió miles de veces en llamadas realizadas a teléfonos de todo el país, y marcaba el comienzo de una estafa que ha crecido exponencialmente en estos tiempos de pandemia. Es la conocida estafa telefónica denominada "phishing", o más actualmente "vishing", ya que es un engaño realizado por medio de una llamada por voz.

¿De qué delito hablamos? Dentro del género de las estafas podemos encontrar diversas modalidades. El Art 172 del Código Penal establece que hay estafa cuando alguien: "... defraudare a otro con nombre supuesto, calidad simulada, falsos títulos, influencia mentida, abuso de confianza o aparentando bienes, crédito, comisión, empresa o negociación o valiéndose de cualquier otro ardid o engaño.", y luego, el Art 173 enumera diversas situaciones consideradas casos especiales de defraudación, y en su inciso 16 enumera uno aplicable al caso que trataremos aquí: "*El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos.*"

Según Romero Villanueva, citado por el Abog. Pablo Palazzi[1] *"el phishing es una modalidad defraudatoria que consiste en remitir un correo electrónico engañoso a clientes para que revelen información personal —tales como su número de tarjeta de crédito o débito o claves de cuentas bancarias—* a través de sitios web simulados o en una respuesta de correo electrónico". Esta modalidad clásica del denominado "phishing" que viene realizándose desde hace décadas, creció significativamente de la mano de la versión denominada "vishing". En esta variante, el engaño se lleva adelante por medio de una llamada telefónica, a través la cual se gana la confianza de la víctima y se consigue información relevante de ésta para tener acceso a sus cuentas.

Las estafas por medios electrónicos incluyen no sólo fraudes a través de correos electrónicos sino también la suplantación de sitios web corporativos generando páginas que son una copia exacta de la original. Los nombres de dominio usados para engañar suelen tener una letra cambiada. La letra "l" (L minúscula) se cambia por la letra "l" (i mayúscula), y páginas falsas se posicionan como primeras en las búsquedas de Google pagando el posicionamiento, de esta forma cualquier internauta incauto y ansioso cae en la trampa.

Las víctimas en las recientes estafas bancarias:

A priori podemos pensar que la única víctima es el cliente defraudado a quien despojan de sus ahorros y a quien endeudan. Pero un análisis más minucioso nos permite distinguir a distintas víctimas de distintos delitos, todos ellos vinculados

con la misma maniobra.

Por un lado a los clientes de la entidad financiera les sustraen los fondos de sus cuentas, y por el otro, a la propia entidad financiera le solicitan dinero mediante técnicas de suplantación de identidad.

El consumidor:

A esta víctima la despojan de los fondos depositados y custodiados por la entidad financiera, cuya prestación principal es justamente custodiar los mismos.

En este tipo de estafas los clientes muchas veces son engañados fundamentalmente porque desconocen el funcionamiento de los mecanismos de seguridad que los bancos han implementado para las operatorias en línea, o en otros casos, directamente debido a las deficientes medidas de seguridad que las entidades financieras ponen en práctica para evitar fraudes. Todo a pesar de las disposiciones del Banco Central de la República Argentina que así lo establecen[2].

Estamos en presencia de una responsabilidad de carácter objetiva que emerge de la ley 24.240 de defensa del consumidor (art. 40 y 40 bis), ya que existe aquí una relación de consumo y es el Banco quien creó los riesgos a los cuales expone a los consumidores relacionados con las tecnologías escogidas para evitar fraudes[3]. Así lo ha entendido también la Cámara Civil y Comercial de la Plata[4], que en una sentencia sobre la ejecución de un crédito generado por canales digitales sostuvo:"...*se estarían canalizando operaciones de crédito para consumo sujetas a las específicas reglas de orden público de la ley consumeril (art. 65, ley 24.240), entre ellas, las presunciones que debieran interpretarse a favor de los eventuales deudores consumidores"*.

Existe una responsabilidad de la entidad bancaria si las medidas de seguridad adoptadas son inefectivas o se ponen en práctica de forma deficiente, como ocurre en las situaciones de fraudes bancarios que nos convocan. Ya sea que se utilice una clave token, una tarjeta magnética, o una aplicación en el dispositivo móvil del cliente, la responsabilidad derivada de estas tecnologías elegidas por el banco le corresponde a éste, y ante la duda, siempre la interpretación debe ser a favor del consumidor.

En relación a los créditos, es claro que la decisión de otorgarlos por medios electrónicos de esta manera es parte de una política comercial de la entidad financiera, y responsabilidad exclusiva de las mismas. Es claro que priorizan el rápido otorgamiento de créditos por sobre el cumplimiento con las leyes y la seguridad jurídica, pero volveremos a este punto más adelante.

La entidad financiera:

Tal como sostiene parte de la doctrina, como el Abog. Ernesto Liceda, estamos aquí frente a un simple caso de uso de datos identificatorios sin autorización, o de forma ilegítima de parte de los delincuentes, y no de "robo de identidad".

En estos casos estamos frente a una maniobra de suplantación de identidad para engañar así a la entidad financiera que no cuenta con medidas de seguridad suficientes para percatarse del engaño del cual está siendo víctima.

La acción encuadra en la conducta delictiva descrita en el Art. 173 inc. 16 de nuestro Código Penal, que refiere a los supuestos en los cuales la defraudación se realiza mediante sistemas informáticos, como son los accesos ilegítimos con claves obtenidas mediante engaños o mediante diversos dispositivos colocados en los cajeros automáticos para copiar los datos de las tarjetas y grabar las claves ingresadas en el teclado, entre otros.

El menoscabo patrimonial lo sufren las entidades financieras. Son los bancos los engañados para otorgar créditos y transferirlos a cuentas de terceros fuera de su control. Y si asumieran su lugar de víctimas deberían presentarse ante las

autoridades judiciales y denunciar los hechos, aportando la evidencia necesaria obrante en sus registros para encontrar a los delincuentes autores del delito del cual son víctimas.

Pero lamentablemente, los bancos hasta hoy han tomado otra actitud contestando las notas de reclamo mediante Carta Documento con textos muy similares al siguiente:

> ***"Del análisis efectuado sobre operaciones denunciadas, no surgirían anomalías que permitan inferir que las mismas no hayan sido autorizadas por Ud., toda vez que fueron realizadas con el usuario BIP y clave BIP TOKEN que usted tiene activo. A todo evento, se le recuerda que las credenciales de los diferentes canales electrónicos (usuario, clave, tarjeta, PIN y PIL) son personales y su guarda como la del plástico es exclusiva responsabilidad del titular de la misma."***

De esta manera, las entidades financieras desconocen cualquier tipo de responsabilidad sobre la deficiente detección de fraudes, y vuelcan todas las culpas en los clientes a quienes nunca explicó el funcionamiento de las medidas de seguridad. Es común ver que consumidores que nunca habían dado de alta la denominada "clave token" son engañados para generarla y comunicarla a los delincuentes. De esta forma, los hechos que marcan el fraude son: el acceso al home banking desde direcciones IP no usadas anteriormente, la generación de claves nuevas, el alta de nuevas cuentas destino de transferencias, el incremento de los montos para transferencias, la solicitud de adelantos de sueldos y créditos en línea, y finalmente el envío de todo el dinero a las cuentas de terceros recientemente dadas de alta. Todo ocurre en un muy breve lapso de tiempo que deja en evidencia una maniobra de fraude, pero que las entidades financieras no han sido capaces de detectar.

Frente a esta situación, la doctrina coincide en que el crédito no es legítimo. Algunos plantean la nulidad del contrato, y otros la palmaria inexistencia, con similares fundamentos:

a. No existe contrato. Tal como nuestro Código Civil y Comercial establece, el requisito para que exista un contrato es el acuerdo de voluntades manifestado mediante un consentimiento que crea, regula, modifica, transfiere o extingue relaciones jurídicas patrimoniales[5].

b. No hay consentimiento, ya que el mismo requiere una conducta de las partes contratantes que manifiesta la existencia de un acuerdo[6].

c. No hay firma. La existencia de una firma digital permitiría probar la autoría de la declaración de voluntad que obliga al firmante, pero en los casos de contratos por medios electrónicos no estamos frente a una firma digital con efectos equivalentes a los de una firma ológrafa, sino frente a la denominada *"firma electrónica",* que no goza de las mismas presunciones de autoría e integridad. Tampoco goza de la garantía del no repudio que establece la Ley de Firma Digital (Ley 25506).

El daño reputacional:

No es menor el daño reputacional que se genera en el momento en el cual la entidad financiera informa la deuda apócrifa (contraída por los delincuentes y atribuida a los clientes) a la Central de deudores financieros del BCRA y a centrales de información de riesgo crediticio.

Si bien las entidades financieras deben informar las deudas al Banco Central, ésta información inexacta en los casos que tratamos no debe privar a los clientes de la posibilidad de acceder al crédito garantizando la protección de los datos personales (arts. 19, 43 y 75 inc. 32 de la Constitución Nacional).

El Artículo 43, tercer párrafo de la Constitución Nacional consagró el derecho de toda perso-

na a interponer una acción expedita y rápida para tomar conocimiento de los datos a ella referidos y en caso de falsedad de los mismos, para exigir su supresión, rectificación y actualización. La Ley de Protección de Datos Personales ofrece la vía de la acción de habeas data, conforme lo establece en su Art. 14.

La acción de habeas data tiene el objeto de darle una herramienta a la persona interesada para controlar la veracidad de la información sobre su persona y el uso que de ella se haga.

Teniendo en cuenta el daño y la confusión que sobre la persona afectada pueden causar los informes con datos incorrectos, la acción de Hábeas Data se presenta como una vía idónea para corregir los datos obrantes sobre las personas damnificadas por la maniobra de Phishing.

Finalmente, podemos concluir que este tipo de fraudes bancarios tienen un abordaje complejo. Requiere impulsar la investigación penal para encontrar a los autores del delito y establecer con claridad la maniobra, y luego, de ser necesario accionar contra la entidad financiera por varios motivos: recuperar el dinero sustraído y rectificar la información sobre los créditos generados por los delincuentes a nombre de los clientes.

[1] Delitos informáticos. Pablo Andrés Palazzi. 3a ed. Ciudad Autónoma de Buenos Aires. Abeledo Perrot, 2016

[2] Puede consultarse la Comunicación A 3323, la Comunicación A 3682 y la Comunicación A 4272 del Banco Central de la República Argentina.

[3] Puede consultarse fallo de fecha 10-12-2020, Autos: "González, Ana Ester c/ Banco Provincia de la provincia de Buenos Aires s/ medidas cautelares (traba/levantamiento)", Sala3-Cám de Apelaciones en lo Civil y Comercial de La Plata, donde el tribunal sostuvo: "... no cabe duda de que nos encontramos frente a un contrato de consumo, de modo que los principios de protección del consumidor guiarán la apreciación del caso. En tal sentido, la parte más débil de la relación es la aquí actora en tanto destinataria de la utilización de un sistema diseñado por la entidad bancaria, sobre quien pesa el despliegue de todas las salvaguardas que doten de confiabilidad al mismo para su operación electrónica o digital (cajeros automáticos o homebanking)"

[4] Ver autos: BANCO DE LA PROVINCIA DE BUENOS AIRES C/Spindola Sabrina Lorena S/Cobro Ejecutivo. Nº de Receptoría: LP-60295-2019, Nº de Expediente: 126798

[5] CCyC, Art. 957: "Definición. Contrato es el acto jurídico mediante el cual dos o más partes manifiestan su consentimiento para crear, regular, modificar, transferir o extinguir relaciones jurídicas patrimoniales".

[6] CCyC Art. 971: "Formación del consentimiento. Los contratos se concluyen con la recepción de la aceptación de una oferta o por una conducta de las partes que sea suficiente para demostrar la existencia de un acuerdo".

[7] CCyC Art. 288: "Firma. La firma prueba la autoría de la declaración de voluntad expresada en el texto al cual corresponde. Debe consistir en el nombre del firmante o en un signo. En los instrumentos generados por medios electrónicos, el requisito de la firma de una persona queda satisfecho si se utiliza una firma digital, que asegure indubitablemente la autoría e integridad del instrumento."

CIBERFRAUDES EN PANDEMIA: DEFENDIENDO AL CONSUMIDOR

BÁRBARA VIRGINIA PEÑALOZA[1]
Abog (Fac. de Dcho de la UNCuyo). Máster en Abogacía Digital y Nuevas Tecnologías (Universidad de Salamanca).
Vicepresidente 2da de Asociación Derecho Informático Argentina (ADIAR).

Durante la pandemia causada por Covid19 hemos sido testigos tanto del aumento de fraudes digitales, como del surgimiento de nuevas modalidades de dicho delito, ello facilitado por los períodos de aislamiento por todos conocidos. Así, personas que nunca operaron on line, tuvieron que familiarizarse en poco tiempo y con escasos conocimientos, con herramientas tecnológicas y plataformas de e commerce o banca digital[2].

Entre las nuevas formas de fraude podemos destacar una en particular que se ha dado en todo el país. Las víctimas reciben un llamado en el que el interlocutor les asegura ser representante de algún hipermercado, de un organismo estatal, de alguna empresa de juegos de azar, e informa que el contacto es con motivo de que la víctima ha sido ganadora de un premio o acreedora de un beneficio social. En ocasiones el motivo es el pago de un bien que la víctima ha puesto a la venta en alguna plataforma. Una vez anunciado el premio o el beneficio, el delincuente solicita el n° de CBU para transferir el premio, asegurando que no pedirá más datos, seguramente ya se haya hecho con ellos mediante *phishing* o alguna otra maniobra. Simula intentar transferir el premio, pero aduce no poder hacerlo por distintos motivos, porque "se trabó la cuenta", porque se requiere una autorización extra. En algunos casos, incluso simulan ser un representante de la entidad bancaria que guiará a la víctima para sortear el obstáculo que impide la transferencia.

Sea cual sea la excusa, siempre obligan a la víctima a concurrir al cajero y la guían durante todo el proceso por teléfono. Así, esta ingresa al cajero con la llamada activa, y es inducida a realizar ciertas diligencias. Para quienes nunca usaron el servicio de home banking, estas diligencias consisten en generar las credenciales y usuario. Cuando la víctima opera con su banco on line, el delincuente procura obtener las claves para poder modificar las credenciales.

El premio, por supuesto, nunca es depositado e, incluso, en ocasiones se solicita la participación de un tercero, al que se le obliga realizar las mismas diligencias en el cajero.

El resultado es que el delincuente se apodera de la cuenta de la víctima, transfiere el saldo y/o solicita préstamos on line, que las entidades bancarias facilitan sin requisito alguno. Una vez acreditado el préstamo, se transfiere inmediatamente a diferentes cuentas, consumando el delito. Aún cuando las víctimas denuncian inmediatamente el hecho, una vez que dejan de estar cautivas en la comunicación con el estafador, los bancos nada reconocen. El delincuente se queda con el préstamo, el banco lo cobra con altos intereses al consumidor, y la víctima soporta las consecuencias de esta nueva modalidad delictiva.

Relación de consumo

Mediante esta maniobra delictiva el delincuente celebra con el banco, suplantando la identidad del consumidor, un contrato de adhesión a distancia (art 1105 CCyC), el préstamo bancario (art 1408 CCyC), siendo aplicables las disposiciones

relativas a los contratos de consumo. Para su celebración se exige la forma escrita y el consumidor debería obtener una copia (art 1386 CCyC), pues el art. 1389 establece que son nulos los contratos de crédito que no contienen información relativa al tipo y partes del contrato, el importe total de financiamiento, el costo financiero total y las condiciones de desembolso y reembolso.

Si nos atenemos a lo establecido por el art. 288 CCyC, en lo que a la firma del contrato respecta, bien podría considerarse la inexistencia del contrato en tanto es un acto jurídico que adolece de un requisito estructural, la voluntad. Ello porque, según dicho artículo, la firma prueba la autoría de la declaración de voluntad expresada en el texto al cual corresponde y, en el caso de los instrumentos generados por medios electrónicos, el requisito de la firma queda satisfecho si se utiliza una firma digital.

Esta norma concuerda con la Ley 25.506 de Firma Digital que reconoce el empleo de la firma electrónica y de la firma digital y su eficacia jurídica en las condiciones que establece. Así, expresa que cuando la ley requiera una firma manuscrita, esa exigencia también queda satisfecha por una firma digital y, en su art. 7, establece una presunción *iuris tantum*, en tanto se presume, salvo prueba en contrario, que toda firma digital pertenece al titular del certificado digital que permite la verificación de dicha firma. Ahora bien, los préstamos bancarios que se otorgan producto de estos fraudes no son firmados mediante firma digital, sino mediante firma electrónica. La cual, según la citada ley, en caso de ser desconocida, corresponde a quien la invoca acreditar su validez.

Esa firma electrónica no puede atribuirse a la víctima, quien desconoce la contratación y las condiciones del préstamo. El acceso al cajero y la manipulación de los datos bancarios se realizan sin su voluntad, bajo un engaño, en consecuencia al faltar uno de los requisitos estructurales del acto, la voluntad, la nulidad de ese acto jurídico es evidente (arts. 272 y 1014 CCyCN) hasta podría decirse que el acto es inexistente.

Las subsiguientes actividades caen como inválidas, ineficaces, o nulas, en orden a que el vicio de la voluntad, asimismo, infecta la causa de los aparentes actos jurídicos de solicitud de crédito y transferencias a terceros desconocidos por la víctima (art. 281 CCyCN), operados desde la suplantación de identidad de la víctima, facilitada por la falta de medidas de seguridad adoptadas por las entidades bancarias.

Responsabilidad de las entidades bancarias

Aún cuando se pretenda endilgar las consecuencias al consumidor, fundándose en una marcada negligencia en su actuar, lo cierto es que la masividad de estas estafas ha proliferado ante la falta de medidas de seguridad bancaria. Por ello, puede afirmarse que los bancos deben responder ante los usuarios que resultan expuestos a estas maniobras. La responsabilidad de carácter objetiva de las entidades bancarias emerge de los arts. 40 y 40 bis de la L.D.C., son estas mismas quienes crean los riesgos que surgen de la utilización de una tarjeta magnética, token y home banking, y la omisión de cumplir con normas mínimas de seguridad, en pos de mayores beneficios y de la posibilidad de solicitar “préstamos online” sin mayores requisitos. Esta operatoria, creada unilateralmente por la entidad bancaria, deja expuestos a los usuarios y allana el camino de los delincuentes.

El deber de seguridad impuesto al proveedor, no se circunscribe sólo a los servicios prestados o a los productos comercializados, sino que debe prevalecer durante toda la relación de consumo. El proveedor debe garantizar la indemnidad a los consumidores.[4] Congruente con ello, el BCRA ha establecido y reiterado en su normativa, la imposición a los Bancos de contar con "mecanismos de seguridad informática" que garanticen la confiabilidad de la operatoria (Comunicación A 3323, 1.7.2.2., último párrafo; Comunicación A 3682, 4.8.6.2; Comunicación A 4272, 2.1.1.6).

En este sentido, la Ley 26.637 en su artículo 2 inc. C exige como medidas mínimas de seguridad que deben adoptar las entidades la utilización de inhibidores o bloqueadores de señal que impidan el uso de teléfonos celulares en el interior de estas. La Comunicación "A" 5575 2.11 del 20/1/11, reglamentó dicha ley y exigió un cronograma de cumplimiento de las Medidas Mínimas de Seguridad en Entidades Financieras para las sucursales bancarias radicadas en el Gran Mendoza. En 2018, la Comunicación "A" 6438 pto.2.11, vuelve a establecer que las entidades deberán adoptar los medios conducentes a hacer operativa la prohibición legal prevista por el inciso c) del artículo 2° de la Ley 26.637 en cuanto al uso de telefonía móvil, como previamente el BCRA lo había hecho en 2017 mediante la Comunicación 6272 pto. 2.11. Ello claramente no se ha cumplido, pues las víctimas ingresan al cajero automático con cautivas en una llamada que permanece activa.

Los bancos tampoco han tomado medidas de seguridad para verificar efectivamente la identidad de quien solicita un préstamo *on line*, o para predecir y detectar acciones inusuales en las cuentas, atendiendo al uso normal que el usuario despliega en su cuenta. Por su parte, los usuarios tampoco pueden anoticiar a las entidades del fraude, pues los canales de comunicación que brindan los bancos no se encuentran activos durante los fines de semana, a pesar de que el servicio on line y la posibilidad de solicitar este tipo de préstamos express sigue vigente en días y horas inhábiles. Claramente, los delincuentes eligen estas ocasiones para cometer el delito.

Juez competente

Tratándose de una relación de consumo, por el art. 53 de la L.C.D., resulta exclusivamente competente la justicia ordinaria.

Las reglas atributivas de la competencia en razón de la materia, tienen por fin asegurar la mejor eficacia y funcionamiento del servicio de justicia con fundamento en el interés general, y son de orden público[5]. Asimismo, como señala la doctrina, los procesos en materia de consumo deben estar orientados a brindar una especial protección a aquel que por fuerza de los hechos se encuentra en desventaja -también- al momento de acceder a la actividad judicial[6]. Esa es la razón por la que el legislador ha declarado improrrogable la competencia cuando se trata de un proceso de consumo y la cláusula de prórroga de jurisdicción se tiene por no escrita (art. 1109 CCyC).

Se han suscitado cuestiones de competencia en ciertos casos donde el proveedor es el Banco de la Nación Argentina, ente autárquico del Estado Nacional. Se alega que es competente la justicia federal, en función de lo establecido por el artículo 116 CN, que establece que corresponde a la CSJN y a los Tribunales Inferiores de la Nación el conocimiento y decisión de los asuntos en que la Nación sea parte. La Carta Orgánica del Banco de la Nación Argentina (Ley 21.799) en su art. 27 establece que, como entidad del Estado Nacional, el Banco Nación está sometido exclusivamente a la jurisdicción federal. Al respecto, la jurisprudencia tiene dicho que corresponde a la Justicia Federal entender en las causas en las que la Nación o una entidad nacional sea parte por aplicación del principio que establece que en presencia de un interés nacional incumbe en términos generales la competencia del citado fuero (SCBA Ac 84578 S del 23/12/02, JUBA B 26788).

Es necesario tener en cuenta que la competencia en razón de la persona es esencialmente prorrogable y que en los casos bajo análisis, el Banco de la Nación Argentina reviste el carácter de proveedor en la relación de consumo, en los términos del art. 2 de la ley de Defensa del Consumidor (L.D.C.) Aquí no hay un interés nacional, sólo el interés individual de un consumidor que se ve severamente afectado y que es el sujeto débil en la relación. Es claro que estamos ante una relación de consumo regida por la L.D.C., de orden público, sin perjuicio de que el proveedor, por la actividad que desarrolle, esté alcanzado asimismo por otra normativa específica.

Concluyendo

Más allá de la denuncia penal del fraude y la investigación que se lleve a cabo, lo cierto es que el consumidor queda desprotegido ante esta situación, puesto que debe pagar por años y con altos intereses las cuotas de un préstamo que no contrató ni percibió. Por su parte el Banco, que incumple con las medidas de seguridad impuestas tanto por la L.D.C. como por la Ley 26.637, cobra estas cuotas enriqueciéndose en virtud de una causa ilícita. Por ello, se hace indispensable, ante la comisión de estos hechos, la inmediata protección del consumidor, quien tiene derecho, por su condición de parte más débil, a un proceso especial de consumo, de tramite ante la justicia ordinaria, única competente en estos casos, y que resuelva atendiendo a los principios fundamentales de la Defensa del Consumidor: la interpretación más favorable, tanto de la ley aplicable, como de la relación de consumo en la que se ve involuntariamente involucrado; y el in dubio pro consumidor.

Más allá de cómo se resuelvan en los tribunales estos casos, se hace fundamental exigir a las entidades bancarias, el efectivo cumplimiento de medidas de seguridad robustas y acordes a los tiempos que corren.

[1] Abog (Fac. de Dcho de la UNCuyo). Máster en Abogacía Digital y Nuevas Tecnologías (Universidad de Salamanca).
Vicepresidente 2da de Asociación Derecho Informático Argentina (ADIAR).

[2] https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2020/Un-informe-de-INTERPOL-muestra-un-aumento-alarmante-de-los-ciberataques-durante-la-epidemia-de-COVID-19 .

[3] Ha dicho la Sala III de la de la Cma. Seg. de Apel. en lo C.y C. de La Plata: Al respecto, esta sala coincide con lo dictaminado por el Sr. Fiscal de Cámaras en tanto expresa que "Prima facie, para una cuenta bancaria utilizada habitualmente a fin de percibir haberes previsionales, que el sistema adoptado por la institución bancaria permita en 24 horas obtener una clave,contraer un préstamo por $ 500.000, transferirlo a cuentas no vinculadas y con las que antes no se han efectuado transacciones, requerir un adelanto de haberes por $ 26.000 y extraerlo todo en forma no presencial, a criterio del dicente no constituye un sistema seguro."

[4] Suprema Corte de Justicia de Mendoza, 26-07-2002 LS310 - Fs.058. En igual sentido, Tercera Cámara de Apelaciones en lo Civil, Comercial, Minas de Paz y Tributario de Mendoza, en causa “Calabró Martín Alejandro c/ Jumbo Retail Argentina SA- Super Vea p/ D y P (accidente de tránsito)” 3/10/16.

[5] (CSJN Fallos: n° 306-2101; 306- 1223 y 1615, n° 314-110)

[6] BRAMUZZI, GUILLERMO CARLOS. Procesos en materia de consumo. 18 de Mayo de 2017. Id SAIJ: DACF170239. www.saij.gob.ar