OPERACIÓN Y USO DE HERRAMIENTAS DE PRIVACIDAD Y ANONIMATO EN ARGENTINA

DRA. JOHANNA CATERINA FALIERO
DR. RODRIGO SEBASTIAN IGLESIAS

DERECHOS DIGITALES
América Latina

INFORME DE INVESTIGACIÓN OPERACIÓN Y USO DE HERRAMIENTAS DE PRIVACIDAD Y ANONIMATO EN ARGENTINA

DRA. JOHANNA CATERINA FALIERO
DR. RODRIGO SEBASTIAN IGLESIAS

@ | DERECHOS DIGITALES
América Latina

Portada y diagramación: Javiera Méndez
Correcciones por Sebastian Alburquerque
Noviembre de 2018.

Esta publicación fue posible gracias al apoyo de Open Technology Fund

Derechos Digitales es una organización independiente y sin fines de lucro, fundada en el año 2005 y cuya misión es la defensa, promoción y desarrollo de los derechos fundamentales en el entorno digital, desde el interés público. Entre sus principales ejes de interés está la defensa y promoción de la libertad de expresión, el acceso a la cultura y la privacidad.

Índice

Abstract / Resumen Ejecutivo

El presente informe de investigación persigue el abordaje integral del marco legal vigente relativo a la operación y utilización de herramientas de privacidad y anonimato en Argentina, tales como la red Tor. Para ello se recorrerá su regulación, enfoque jurisprudencial y evolución doctrinaria a nivel nacional, y así se responderá a los interrogantes jurídicos que se suscitan y las problemáticas en torno a su legalidad, privacidad, monitoreo, utilización como evidencia, responsabilidad, etc., y proveer así conclusiones y reflexiones que sirvan como aporte para su futura recepción normativa a nivel local.

Introducción

Con el surgimiento, masificación y generalización del uso de las tecnologías de la información y la comunicación, los datos, su protección y la privacidad de los individuos se han convertido en los capitales intangibles más preciados del individuo. No sólo se ha multiplicado la cantidad de datos que transmitimos y su velocidad, sino también lo han hecho las diversas formas de vulnerar su privacidad y seguridad.

Los derechos a la protección de datos, privacidad, seguridad, intimidad, autodeterminación informativa y libertad de expresión, son derechos humanos fundamentales reconocidos así por numerosísimos tratados internacionales, así como por regulaciones de tipo regional y local. Por ello, ha surgido la necesidad técnica de acompañar ese cúmulo de derechos con herramientas prácticas que sirvan para el ejercicio de los mismos en línea.

Es así como de manera progresiva han surgido diversas herramientas de privacidad y anonimato –tales como la red Tor– que se utilizan para evitar las vulneraciones a la privacidad, la trazabilidad y el monitoreo, por parte tanto del sector privado como gubernamental. Su utilización con el correr del tiempo se ha ido ampliando progresivamente, y es allí donde comenzaron a surgir los primeros ecos internacionales de las problemáticas, dilemas e interrogantes jurídicos en torno a su uso, así como también sus primeras recepciones jurisprudenciales, doctrinarias y regulatorias, las cuales no han sido del todo favorables a su acogida.

El presente trabajo de investigación procura efectuar un abordaje integral que recorrerá la regulación legal existente en Argentina en torno a las temáticas de privacidad, anonimato, seudonimia y cifrado, y también sobre la operación y utilización de herramientas tales como Tor, su enfoque doctrinario y jurisprudencial.

A su vez, se estudiará el enfoque en materia de responsabilidad legal respecto de la intermediación en servicios relacionados, así como la posibilidad de su prohibición y problemáticas jurídicas subyacentes a su operatoria en el país, y la opinión jurisprudencial y doctrinaria mayoritaria vigente a la fecha.

Por último, se analizarán los extremos legales relativos a la monitorización de datos por parte de las autoridades estatales, y los requisitos necesarios para poder hacer uso de estas herramientas en materia de evidencia digital en el ámbito penal, para investigación u obtención de prueba en el marco de procesos legales.

Por todo ello cabe concluir anticipadamente que resulta necesario, no sólo a nivel local, sino regional y global, efectuar un serio y robusto abordaje interdisciplinario en estas temáticas, que permita fundar una regulación orientada principiológicamente a la preservación de los derechos individuales en pugna y con miras a la evitación y prevención de sus utilizaciones desviadas, entendiendo la privacidad como bien jurídico supremo a proteger en la era digital moderna.

Desarrollo

I. Privacidad, anonimato, confidencialidad, seudonimia, y cifrado: regulación y abordaje en Argentina.

El derecho a la intimidad y a la privacidad han sido reconocidos en nuestro país como derechos de carácter constitucional, personalísimo y fundamental. Nuestra Constitución Nacional reconoce los derechos a la intimidad y privacidad por medio de sus Arts. 18, 19 y 33, y por medio de los Tratados Internacionales en Derechos Humanos, incorporados al bloque constitucional en la Reforma de 1994 en el Art. 75 Inc. 22., a saber los siguientes: la Declaración Americana de los Derechos y Deberes del Hombre; la Declaración Universal de Derechos Humanos; la Convención Americana sobre Derechos Humanos; y el Pacto Internacional de Derechos Civiles y Políticos y su Protocolo Facultativo.

El Art. 18 de la Constitución Nacional consagra, entre otras cosas, la inviolabilidad del domicilio, de la correspondencia epistolar y los papeles privados: *"Art. 18.-… El domicilio es inviolable, como también la correspondencia epistolar y los papeles privados; y una ley determinará en qué casos y con qué justificativos podrá procederse a su allanamiento y ocupación. …"*

El Art. 19 establece el principio de reserva por el cual se enuncia: *"Art. 19.- Las acciones privadas de los hombres que de ningún modo ofendan al orden y a la moral pública, ni perjudiquen a un tercero, están sólo reservadas a Dios, y exentas de la autoridad de los magistrados. Ningún habitante de la Nación será obligado a hacer lo que no manda la ley, ni privado de lo que ella no prohíbe."*

El Art. 33 que reconoce constitucionalmente los derechos implícitos, dice: *"Art. 33.- Las declaraciones, derechos y garantías que enumera la Constitución no serán entendidos como negación de otros derechos y garantías no enumerados; pero que nacen del principio de la soberanía del pueblo y de la forma republicana de gobierno."*

La primera regulación en torno de la protección de los datos personales en el sistema normativo argentino ha sido el juego del Art. 33, protección de datos personales como un derecho implícito, Art. 19 –principio de reserva– y Art. 18 –inviolabilidad del domicilio, la correspondencia y los papeles privados- ya citados, de nuestra Constitución Nacional, y por medio del Art. 1071 bis del entonces CCNA – Código Civil de la Nación Argentina -, el que fuera reemplazado por el actual Art. 1770 del CCyCNA – Código Civil y Comercial de la Nación Argentina, por vía de la regulación del derecho a la intimidad, artículo que expresa: *"Art. 1770.- Protección de la vida privada. El que arbitrariamente se entromete en la vida ajena y publica retratos, difunde correspondencia, mortifica a otros en sus costumbres o sentimientos, o perturba de cualquier modo su intimidad, debe ser obligado a cesar en tales actividades, si antes no cesaron, y a pagar una indemnización que debe fijar el juez, de acuerdo con las circunstancias. Además, a pedido del agraviado, puede ordenarse la publicación de la sentencia en un diario o periódico del lugar, si esta medida es procedente para una adecuada reparación."*

Tiempo más tarde, con la Reforma Constitucional del año 1994, se incorporó a la Constitución Nacional el Art. 43 en su párrafo tercero, que introduce la figura del hábeas data.

Finalmente, la protección de datos personales en Argentina recibe su regulación específica

con la sanción de la Ley 25326, de Protección de los Datos Personales, reglamentada por el Decreto 1558/2001.

El objeto de la Ley de Protección de Datos Personales 25326 es amplio y referido a la actividad que representa el tratamiento de datos y focaliza su eje protectorio en el derecho humano fundamental de origen constitucional implícito, a saber, el de autodeterminación informativa.

La Ley de Protección de Datos Personales actualmente se encuentra atravesando un proceso que tiene por objeto su reforma. A estos fines y en el marco del Proyecto denominado Justicia 2020, durante el año 2016 se recibieron aportes de los más diversos y prestigiosos representantes de todos los sectores de la sociedad civil (sector privado, gobierno, academia, tercer sector) respecto de los puntos a reformar de la norma. A partir de éstos se elaboró el documento "Ley de Protección de Datos Personales en Argentina. Sugerencias y aportes recibidos en el proceso de reflexión sobre la necesidad de su reforma. Agosto-Diciembre 2016"[1] de la entonces Dirección Nacional de Protección de Datos, ahora denominada Agencia de Acceso a la Información Pública.

En consonancia con estos aportes recibidos se procedió a la redacción de una primera versión del Anteproyecto de Reforma de la Ley de Protección de Datos Personales[2], el que fuera publicado el 1 de Febrero de 2017. Luego de su publicación, y durante el transcurso de ese mismo mes, se recibieron nuevamente aportes críticos de los diversos representantes de todos los sectores de la sociedad civil, a partir de lo cual se elaboró una segunda versión de la redacción del Anteproyecto de Reforma de la Ley de Protección de Datos Personales[3]. A la fecha, ninguno de estos anteproyectos ha tenido tratamiento ni aprobación parlamentaria, por lo que continúan siendo estudiados.

El deber de confidencialidad o reserva, en nuestro sistema jurídico, se desprende como un deber profesional en entornos tales como la relación médico paciente, cliente letrado, y protección de datos. Como ejemplo de ello, nuestra aún vigente Ley de Protección de Datos Personales 25326 dice al respecto en su Art. 10: *"Art. 10. — (Deber de confidencialidad). 1. El responsable y las personas que intervengan en cualquier fase del tratamiento de datos personales están obligados al secreto profesional respecto de los mismos. Tal obligación subsistirá aun después de finalizada su relación con el titular del archivo de datos. 2. El obligado podrá ser relevado del deber de secreto por resolución judicial y cuando medien razones fundadas relativas a la seguridad pública, la defensa nacional o la salud pública."*.

Por otra parte, el anonimato y la privacidad por seudonimia, no se encuentran reconocidos ni regulados aún como derecho, y por el contrario se encuentran en términos generales combatidos debido a las dificultades que estas técnicas de privacidad representan para la práctica forense y la persecución e investigación de delitos tanto en el plano tradicional como el digital. Sin perjuicio de la visión negativa que pesa sobre ellos, no son prácticas

---

1 "Ley de Protección de Datos Personales en Argentina. Sugerencias y aportes recibidos en el proceso de reflexión sobre la necesidad de su reforma. Agosto-Diciembre 2016" Disponible en: https://www.argentina.gob.ar/sites/default/files/documento_aportes_reforma_ley25326_0.pdf

2 Primera versión del Anteproyecto de Reforma de la Ley de Protección de Datos Personales. Disponible en: https://www.argentina.gob.ar/sites/default/files/anteproyecto_de_ley_de_proteccion_de_los_datos_personales.pdf

3 Segunda versión del Anteproyecto de Reforma de la Ley de Protección de Datos Personales. Disponible en: https://www.argentina.gob.ar/sites/default/files/anteproyecto_reforma_ley_proteccion_de_los_datos_personales_nueva_version.pdf

estrictamente prohibidas desde lo normativo, por lo que, si bien pueden actuar en ocasiones como prueba indiciaria a nivel judicial en contrario de quien las utilice, en la realidad no existe prohibición legal alguna en torno a las mismas.

Finalmente, en lo que respecta al cifrado como técnica de protección y privacidad de datos, nuestro sistema protectorio en materia de datos personales se pronuncia a favor de la misma, en la Disposición 11/2006 de la entonces Dirección Nacional de Protección de Datos Personales, específicamente en lo relativo a las medidas de seguridad de carácter critico aplicables en materia de tratamiento de datos. El punto 4 en materia de medidas críticas prescribe específicamente lo siguiente en cuanto a la transmisión de datos sensibles: *"4. Transmisión de datos: los datos de carácter personal que se transmitan a través de redes de comunicación, deberán serlo cifrados o utilizando cualquier otro mecanismo que impida su lectura y/o tratamiento por parte de personas no autorizadas."*

II. Libertad de expresión y prohibición de la censura previa.

El marco regulatorio Interamericano protege de manera robusta y amplia las libertades de pensamiento y expresión, en la Convención Americana y su Art. 13, el que expresa que toda persona tiene derecho a estas libertades, lo que comprende *"la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección"* (Inc. 1), y prescribe en lo específico que su ejercicio *"no puede estar sujeto a previa censura sino a responsabilidades ulteriores, las que deben estar expresamente fijadas por la ley y ser necesarias para asegurar: a. el respeto a los derechos o a la reputación de los demás, o b. la protección de la seguridad nacional, el orden público o la salud o la moral públicas."* (Inc. 2).[4]

A su vez, por medio de la Declaración Americana de los Derechos y Deberes del Hombre[5], los protege en su Art. IV, el que dice: *"Derecho de libertad de investigación, opinión, expresión y difusión. Toda persona tiene derecho a la libertad de investigación, de opinión y de expresión y difusión del pensamiento por cualquier medio."*, y por medio de la Carta Democrática Interamericana[6], que formula en el primer párrafo de su Art. 4 que *"Son componentes fundamentales del ejercicio de la democracia la transparencia de las actividades gubernamentales, la probidad, la responsabilidad de los gobiernos en la gestión pública, el respeto por los derechos sociales y la libertad de expresión y de prensa."*

La libertad de pensamiento y expresión[7] ya era reconocida por nuestro país en el texto de

---

4 "Convención Americana Sobre Derechos Humanos". Suscrita en la Conferencia Especializada Interamericana Sobre Derechos Humanos (B-32), San José, Costa Rica 7 al 22 de noviembre de 1969, disponible en: https://www.oas.org/dil/esp/tratados_B-32_Convencion_Americana_sobre_Derechos_Humanos.htm

5 "Declaración Americana de los Derechos y Deberes del Hombre", IX Conferencia Internacional Americana, disponible en: http://www.oas.org/es/cidh/mandato/Basicos/declaracion.asp

6 "Carta Democrática Interamericana", Vigésimo Octavo Período Extraordinario de Sesiones, 11 de septiembre de 2001, Lima, Perú, disponible en: http://www.oas.org/charter/docs_es/resolucion1_es.htm

7 Véase, Laplacette, Carlos José, "Libertad de expresión ¿derecho individual o colectivo? Sup. Const. 2014 (agosto), 25/08/2014, 17 - LA LEY2014-E, 642.

su Constitución[8] histórica, en su Art. 14, que en lo pertinente reconoce a sus habitantes el derecho de "*publicar sus ideas por la prensa sin censura previa*" y se complementa con lo dispuesto por el Art. 32 del mismo cuerpo, el que fue incorporado en su reforma en 1860, el que ordena que *"El Congreso federal no dictará leyes que restrinjan la libertad de imprenta o establezcan sobre ella la jurisdicción federal."*. Por su parte, tiempo más tarde, la reforma constitucional del año 1994, que incorporó a nuestro texto numerosos tratados internacionales de derechos humanos por medio del Art. 75 Inc. 22, ensanchó el bloque de constitucionalidad y solidificó el reconocimiento de este derecho.

En particular y en lo referente a contenidos de Internet, la sanción de la Ley 26032[9] reconoció expresamente desde el año 2005 que *"La búsqueda, recepción y difusión de información e ideas de toda índole, a través del servicio de Internet, se considera comprendido dentro de la garantía constitucional que ampara la libertad de expresión."*

En lo atinente a las restricciones que nuestra regulación recepta en torno a estas libertades, se encuentran aquellas que efectúan nuestro Código Civil y Comercial[10] y nuestro Código Penal[11].

El código civil Veleciano[12] modificado en el año 1968 incorporó en su Art. 1071 la figura del abuso del derecho, mientras que tiempo más tarde en 1975 incorporó en su Art. 1071 Bis una restricción expresa a la libertad de expresión, que constituye un ilícito de tipo civil.[13] El texto de ese artículo Original rezaba lo siguiente: *"El que arbitrariamente se entrometiere en la vida ajena, publicando retratos, difundiendo correspondencia, mortificando a otros en sus costumbres o sentimientos, o perturbando de cualquier modo su intimidad, y el hecho no fuere un delito penal, será obligado a cesar en tales actividades, si antes no hubieren cesado, y a pagar una indemnización que fijará equitativamente el juez, de acuerdo con las circunstancias; además, podrá éste, a pedido del agraviado, ordenar la publicación de la sentencia en un diario o periódico del lugar, si esta medida fuese procedente para una adecuada reparación."*. Nuestro Código Civil fue modificado y unificado en el año 2014 con el Código Comercial, dando nacimiento al actual código vigente – el que denominamos Código Civil y Comercial - por medio del texto aprobado por la Ley 26994. En este régimen, contamos con el Art. 1770, el que ya fuera citado previamente en referencia a la protección del derecho a la intimidad y privacidad de las personas.

---

8 Constitución de la Nación Argentina. Ley Nº 24.430, disponible en: http://servicios.infoleg.gob.ar/infolegInternet/anexos/0-4999/804/norma.htm

9 Ley 26.032 - Servicio De Internet. Establécese que la búsqueda, recepción y difusión de información e ideas por medio del servicio de Internet se considera comprendida dentro de la garantía constitucional que ampara la libertad de expresión, sancionada: Mayo 18 de 2005, promulgada de hecho: Junio 16 de 2005, disponible en: http://servicios.infoleg.gob.ar/infolegInternet/anexos/105000-109999/107145/norma.htm

10 Ley 26994 - Código Civil y Comercial de la Nación, sancionada: Octubre 1 de 2014, promulgada: Octubre 7 de 2014, disponible en: http://servicios.infoleg.gob.ar/infolegInternet/anexos/235000-239999/235975/texact.htm

11 Ley 11.179 (T.O. 1984 actualizado) - Código Penal de la Nación Argentina, disponible en: http://servicios.infoleg.gob.ar/infolegInternet/anexos/15000-19999/16546/texact.htm

12 Ley 340 - Código Civil de la Nación, disponible en: http://servicios.infoleg.gob.ar/infolegInternet/anexos/105000-109999/109481/texact.htm

13 *Véase*, Gaibrois, Gustavo L., "El daño moral ocasionado por la libertad de expresión y el Proyecto de Código Civil y Comercial de la Nación.", DFyP 2013 (noviembre), 01/11/2013, 261.

Desde lo penal, el Código respectivo se ocupa de sancionar los delitos de acción privada de calumnias e injurias, en su Título II "*Delitos Contra el Honor*", que se diferencian en términos muy generales – unas de otras – en que las primeras refieren a la falsa imputación a una persona de la comisión de un delito determinado, mientras que las segundas aluden a expresiones realizadas sobre una persona que lesionen su dignidad, honor, estima, reputación, etc., que no constituyan la comisión de un ilícito.

III. Legalidad y *leading case* judicial respecto a las herramientas de privacidad y anonimato.

En Argentina, a la fecha, no existe ninguna norma específica relativa a la utilización de herramientas de privacidad y anonimato. Por lo que la utilización de herramientas tales como Tor no se encuentra expresamente prohibida en nuestro sistema jurídico.

Es práctica generalizada, tanto en entornos de privacidad, como en aquellos usuarios conscientes y rigurosos respecto de su privacidad y la protección de sus datos, volcarse a la utilización de herramientas de privacidad y anonimato.

La creciente concientización y educación existente en nuestra población, respecto de los peligros que afrontamos de manera exponencial en nuestra privacidad, intimidad, seguridad y protección de datos, conlleva correlativamente a que se divulgue y expanda la utilización de estos servicios.

Por otra parte, desde un punto de vista forense y en lo relativo específicamente a la investigación en cibercriminalidad, la utilización de estas herramientas dificulta naturalmente la persecución en materia de autoría y trazabilidad de los ilícitos en el ámbito digital. Esto motiva a que la utilización de las mismas sea naturalmente mal vista por ciertos sectores, judiciales y de prevención de ilícitos, los que se ven expuestos en la actualidad al desafío permanente en su actualización en lo relativo a técnicas de investigación forense, ya que las técnicas y protocolos tradicionalmente utilizados no sirven como respuesta para los nuevos entornos y desafíos que plantean estas herramientas.

A nivel nacional, el *leading case* –que data del año 2016– en lo relativo a la utilización de esta tipología de herramientas, fue el caso de Iván Barrera Oro, alias "Hackan", quien producto a una denuncia efectuada por 4Chan en NCMEC (*National Center for Missing & Exploited Children*), fue perseguido judicialmente por un presunto tráfico de una imagen de pornografía infantil en Agosto de 2013, ya que el mismo poseía un nodo de salida de Tor funcionando en su domicilio.

Como resultado de este proceso, se comprobó la inocencia del imputado, demostrando finalmente no sólo que las herramientas investigativas y procedimientos forenses requerían urgentemente de un *aggiornamiento* para adecuarse a la nueva realidad que plantean estas herramientas de privacidad y anonimato, sino que estas últimas no se encuentran prohibidas en nuestro país.

Iván Barrera Oro fue investigado durante algo más de un año por la publicación de una imagen de pornografía infantil publicada en la web 4chan.org en el año 2013[14] y que un usuario

---

14 10/08/2013 fue la fecha de la publicación.

denunció en el sitio y éste se vio obligado a denunciar en el año 2015[15]. Luego, recién el 16 de Junio de 2016 se realizó el allanamiento respectivo y secuestro de todos los dispositivos electrónicos informáticos y de almacenamiento del imputado.

Iván Barrera Oro fue imputado por el delito de producción y distribución de pornografía infantil y participó de la pericia informática pertinente. En función de colaborar con la investigación efectuó la entrega de su llave físico – lógica para solamente abrir el HD (*hard disk*) del equipo incautado en el allanamiento, que había funcionado como TOR Exit Node de nombre "BradleyManning"[16] hasta mediados del año 2015, con el objetivo de corroborar y certificar que ese era el HD y que el Exonerator estaba en lo correcto.

Como fue coherente el resultado de la pericia con la inocencia del imputado y cuando ya la causa estaba a punto de prescribir en su etapa de investigaciones (Instrucción), la defensa solicitó el sobreseimiento de Iván Barrera Oro[17]. El Fiscal Javier Martin Lopez Zavaleta informó que la investigación se encontraba en curso[18] y el Juez Carlos Aostri solicitó un pedido de antecedentes penales[19], ambos hechos con la finalidad de forzar la prescripción de la acción.

Al negar la audiencia obligatoria de la cual se había solicitado el correspondiente sobreseimiento (y apelado su negativa por parte del Fiscal a fojas 234), no restó otra alternativa al tribunal que dividir la sentencia en dos partes, la primera donde indicó la prescripción de la investigación[20] y la segunda donde otorgó el sobreseimiento[21] solicitado por la defensa de Iván Barrera Oro, concluyendo así cualquier reclamo por la falta de audiencia, y dejando al primer TOR Exit node sin siquiera antecedentes penales por el proceso en su contra, además de dejar abierta la vía civil para la reparación integral por los daños y perjuicios soportados.

Por todo ello y conforme a los antecedentes, las herramientas de privacidad y anonimato, tales como Tor, son lícitas, no evitan los ilícitos, como así tampoco los causan, sino que simplemente son herramientas al auxilio del individuo en defensa de sus derechos humanos, como mecanismos auxiliares de garantizar su libertad de expresión, intimidad, privacidad y confidencialidad de las comunicaciones.

---

15 06/07/2015 a las 04:00:00 UTC recibido por NCMEC, en Argentina aún era domingo 05/07/2015.

16 Informado a Fojas 97 del expediente, en la declaración de Barrera Oro "... Es claro que la persona que se encuentra tras el sobrenombre de Bradley Manning (nickname) soy yo, dado que encuentran mi dirección IP y las fechas correspondiente, de haber realizado la investigación de forma seria observarían que no se puede tardar 3 años en realizar un allanamiento y no tener en cuenta en ningún momento que cualquier dirección IP puede ser Nodo de Salida de la Red TOR, también se tiene que ingresar a https://collector.torproject.org/ para saber si en ese momento exacto estaba siendo utilizado mi Nodo de TOR o era en verdad yo quien estaba realizando la navegación, una vez más colocando mi dirección IP pueden corroborar que en esa hora y fecha estaba funcionando mi Nodo de Salida de TOR...".

17 A fojas 231, "... Que según los resultados periciales obtenidos a fecha 5 de julio de 2017 y atendiendo a la investigación cursada sobre mi persona solicito tener a bien dicte el correspondiente sobreseimiento en función del artículo 195 inc. C por falta de participación criminal del imputado respecto de la conducta descripta en el decreto de determinación del hecho...".

18 A fojas 233, "... Que esta parte no ha decidido hasta el momento adoptar temperamento alguno respecto de la situación procesal del encausado.... Entiendo que la petición de sobreseimiento resulta cuando mas prematura para esta etapa de la investigación...".

19 A fojas 234, "...actualice los antecedentes del imputado...".

20 A fojas 243 "... declarar extinguida la acción penal acaecida por prescripción en favor de Iván Barrera Oro...".

21 A fojas 243 Vuelta "... sobreseer a Iván Barrera Oro de las demás condiciones obrantes en autos por la presente causa respecto del hecho acaecido el 10 de agosto de 2013".

IV. Herramientas de privacidad y anonimato como mecanismos para evitar la censura previa de contenidos.

Internet como sinónimo de comunicación global y convergencia, permite la publicación masiva de contenidos –información y datos de toda índole y especie-, que pueden ser accedidos y consultados, sin limitantes temporales ni geográficas, por usuarios de todas partes del mundo. Estadísticas realizadas en el año 2015, por Ben Walker de Voucher Cloud[22], arrojaron cifras impactantes en lo que respecta a la capacidad de generación de contenidos que posee Internet, proyectada para este año en 50 mil gigabytes por segundo. Todo ello nos permite afirmar con total certeza que no existe otro medio alternativo de amplitud y magnitud semejante en nuestros días en términos informativos y comunicacionales, motivo por el cual se justifica su protección y regulación.

En la generación de contenidos, independientemente del soporte y medio utilizado para el mismo, se plasma –entre muchos otros derechos humanos fundamentales mencionables- básicamente el derecho a la libertad de pensamiento y de expresión, y la prohibición de la censura previa, derechos previamente examinados de manera frondosa.

Dentro de los peligros que enfrenta nuestra sociedad digital, se erige la remoción indiscriminada, irrazonable o injustificada de contenidos en Internet, que se presenta como amenaza severamente ostensible a la libertad de expresión y pensamiento. Los derechos que se encuentran en jaque a través de esta práctica han inspirado su estudio exhaustivo, con el objetivo final de poder encontrar el modo de limitarla para que, en caso de requerirse, cumpla su finalidad y a su vez, no restrinja derechos que son la misma base sobre la cual se edifican los regímenes democráticos modernos. Es por esto que como base de todo análisis se tiene que verificar que la remoción de contenidos sea compatible con el principio democrático, es decir, adecuada a las exigencias de la sociedad democrática

En el entorno digital, la remoción de contenidos es la medida más radical que enfrenta la libertad de expresión, porque implica lisa y llanamente que la información que se ha removido deje de circular. Es decir, que nadie más pueda acceder a la misma. Por lo que la remoción de contenidos debe ser interpretada restrictivamente, del mismo modo que propone el Sistema de Protección Interamericano, el que elaboró a través de su jurisprudencia y estándares un "Test Tripartito", el que consiste en comprobar en cada caso en particular, que la limitación a la libertad de expresión sea legítima, y por ello admisible.

El Sistema de Protección Interamericano propone, en primer lugar, verificar su legalidad; en segundo lugar, su necesidad; y en tercer lugar, su proporcionalidad, es decir, la adecuación y justificación o racionalidad de los medios utilizados para el cumplimiento de los fines perseguidos. Solamente si la remoción de un contenido web atraviesa este testeo, se encuentra justificada. De lo contrario, se podría estar vulnerando la libertad de expresión y hasta se podría llegar a incurrir en censura.

La censura previa se encuentra prohibida por el Sistema Interamericano de Protección de Derechos Humanos, dirección que han seguido prácticamente todas las regulaciones regio-

---

22 *Véase*, VCloudNews, "Every Day Big Data Statistics - 2.5 Quintillion bytes of data created daily", 5 de Abril de 2015, disponible en: http://www.vcloudnews.com/every-day-big-data-statistics-2-5-quintillion-bytes-of-data-created-daily/

nales a nivel constitucional, puesto que constituye la restricción más palmaria y absoluta a las libertades de pensamiento y expresión.

En el mundo digital, la censura previa restringe el potencial social de Internet como canal de expresión[23], clave en los regímenes democráticos, y más aún en aquellos lugares del mundo donde no impera la democracia o la misma se encuentra en crisis, supuestos en los que en ocasiones se constituye como el único medio y canal disponible de expresión de la sociedad.

La remoción arbitraria de un contenido, implica un acto de censura previa online, que puede ser desplegado ya sea de modo técnico[24] o de manera directa. De allí la preocupación que ha crecido en torno a la potestad irrestricta, unilateral o sin regulación, de remoción de contenidos de los intermediarios de Internet[25], que dio lugar a la elaboración de los llamados "Principios de Manila"[26]. Estos proporcionan una guía de buenas prácticas que sirven a los fines de promover la libertad de expresión e innovación en Internet y sostienen en líneas generales que las restricciones de contenidos deben ser requeridas por orden judicial, que deben ser claras, inequívocas y respetar el debido proceso y además cumplir con los test de necesidad y proporcionalidad.

La utilización de herramientas de privacidad y anonimato, tales como Tor, pueden ser utilizadas como mecanismos de auxilio del poder de la ciudadanía global y democrática, para evitar los actos de censura previa a los cuales pueden verse expuestos los contenidos online publicados.

No existe al respecto, en nuestro país, ninguna regulación específica que se pronuncie en contrario a su utilización, no obstante ello, nuestro sistema sí se pronuncia firmemente respecto de la prohibición de la censura previa y el derecho a la libertad de expresión y libre circulación de las ideas.

Por lo que, en los entornos digitales citados, donde la remoción de contenidos por medio de la censura previa online puede constituir una amenaza para los valores democráticos que sostienen nuestra sociedad moderna, orientada hacia la garantía del ejercicio de los derechos humanos como valor supremo y fundamental, las herramientas de privacidad y anonimato son mecanismos que coadyuvan al empoderamiento de la ciudadanía digital.

---

23 *Véase,* Sabsay, Daniel Alberto Fernández, Cristian, "La libertad de expresión en la "blogósfera". LA LEY 16/09/2013, 16/09/2013, 12 - LA LEY16/09/2013, 12 - LA LEY2013-E, 251 - RCyS2013-X, 39.

24 *Véase,* Zabale, Ezequiel María, "Neutralidad de la red como garantía de la libertad de expresión.", Sup. Act. 08/03/2012, 08/03/2012, 1.

25 *Véase,* Vaninetti, Hugo A. Vaninetti, Gustavo J., "Responsabilidad de los buscadores y libertad de expresión.", LA LEY 02/03/2014, 02/03/2014, 6 - LA LEY2014-A, 120 - LA LEY03/02/2014, 6 - RCyS2014-IV, 37; y Zunino, Marcos, "La responsabilidad de los proveedores de servicios de Internet y la libertad de expresión.", LA LEY 31/10/2012, 31/10/2012, 1 - LA LEY2012-F, 821 - LLP 2013 (noviembre), 01/11/2013.

26 "Principios De Manila Sobre Responsabilidad De Los Intermediarios." Guía de Buenas Prácticas Que Delimitan la Responsabilidad de los Intermediarios de Contenidos en la Promoción de la Libertad de Expresión e Innovación. Una iniciativa global de la sociedad civil. Versión 1.0, 24 de Marzo de 2015, disponible en: https://www.eff.org/files/2015/06/23/manila_principles_1.0_es.pdf

V. La responsabilidad de intermediarios al operar herramientas de privacidad y anonimato. Su régimen a nivel local.

Existen múltiples modelos de intermediación en Internet, entre los que se pueden mencionar los buscadores, los portales especializados y públicos, los portales corporativos, los portales colaborativos, los foros, las plataformas de subasta, los agentes inteligentes y los portales de mercado.

Entre ellas, los más resonantes a nivel nacional han sido las plataformas de comercio electrónico que sirven para la venta de productos por Internet, las que no se encuentran restringidas a los sitios web de fabricantes exclusivamente. Plataformas de intermediación en comercio electrónico permiten la comunidad entre diversos proveedores y consumidores, y brindan a estos últimos un servicio por el cual pueden adquirir los bienes y servicios allí ofertados.

Los intermediarios de mercado que se dedican al comercio electrónico mayoritariamente generan sus ingresos a través del abono de comisiones, honorarios, cargos, servicios, etc., que les cobran a sus afiliados (vendedores o compradores); de allí que, sin perjuicio de que por lo general se defienden aludiendo la limitación de su actividad a la intermediación de las partes (proveedor y consumidor), resultan solidariamente responsables por los riesgos naturales e inherentes a su actividad, puesto que lucran con ella, lo que típicamente se conoce por el latiguillo jurídico riesgo-provecho.

El factor de atribución de la responsabilidad en actividades de comercio electrónico de proveedor-consumidor es objetivo; sus eximentes son culpa exclusiva de la víctima, responsabilidad de un tercero por el cual no se deba responder, caso fortuito o fuerza mayor; y la responsabilidad de los intermediarios es solidaria, sin perjuicio de las acciones de repetición que existan en el caso (respecto del proveedor, fabricante, distribuidor, marca, transportista, etc.).

Sin perjuicio de que la postura consumerista en la materia sea la precedente, las tres posturas imperantes en la materia son: la tesis de la responsabilidad, irresponsabilidad y responsabilidad subjetiva.

Por una parte, quienes sostienen la aplicabilidad directa del estatuto consumeril a la intermediación en Internet donde participen consumidores, afirman que lo adecuado es la aplicación del factor atributivo objetivo de la responsabilidad de los intermediarios comerciales en las relaciones de consumo. La intermediación en Internet es una actividad riesgosa y lucrativa, por lo que todo aquel que se dedique a ella debe responder por los riesgos inherentes a la misma ante el consumidor, sin perjuicio de las acciones de repetición que pueda ejercer contra aquel que considere responsable en su faz interna relacional (fabricante, proveedor, distribuidor, marca, transportista, etc.).

En segundo lugar, se encuentran quienes sostienen la aplicabilidad del factor subjetivo de la responsabilidad, ya que entienden que de aplicarse el primero la actividad de intermediación comercial se detendría por los insuperables e injustos costos económicos que acarrea la responsabilidad objetiva. La responsabilidad subjetiva recepta como eximentes la ausencia de dolo o culpa, según sea el caso.

Por último, la tercera postura doctrinaria, que resulta la más beneficiosa para el polo empresario, es la tesis de la irresponsabilidad de los intermediarios, puesto que en ella se sostiene

que como estos últimos no son los generadores de la causa del daño (vicio o riesgo), sino que simplemente prestan un servicio de intermediación y acercamiento entre las partes, jamás podrían ser responsabilizadas. Esta postura resulta claramente arbitraria porque desatiende absolutamente al hecho de que los intermediarios lucran con dicha actividad, ya sea por medio de publicidad, ganancias asociadas, comisiones, cargos, honorarios, etc., y omite contemplar otras causales de daños. La postura de la irresponsabilidad omite considerar a la actividad de intermediación como actividad económica riesgosa, lo cual no tiene justificación alguna; la intermediación es una variante más de las actividades económicas que se realizan en el mercado, y como todas ellas, posee sus riesgos y responsabilidades correlativas.

La tesis de la responsabilidad objetiva en donde imperen las relaciones de consumo, por vicios, riesgos de las cosas o de la prestación del servicio, se erige como la respuesta jurídica correcta que atiende a la protección iusfundamental de los derechos de los usuarios y consumidores y que se encuentra receptada por nuestra Constitución Nacional, codificación civil y comercial y ley específica en la materia. El estatuto de protección consumeril aplica con independencia al medio sobre el cual se materializa la relación de consumo. La intermediación de agentes novedosos en la cadena de comercialización por la cual el consumidor adquiere bienes o servicios tampoco obsta a la aplicabilidad de la norma.

Así, recientemente se ha sostenido: "*…una empresa dedicada a la intermediación de compras, ventas y pagos por Internet debe ser multada por infracción a los arts. 4, 9, 11, 13 y 34 de la ley 24.240, en virtud de la denuncia formulada por una usuaria que compró un producto cuya descripción no coincidió con el que le entregó el vendedor, pues, en la medida que cobra por publicitar y por la concreción de las operaciones, deviene responsable en los términos del estatuto del consumidor, ya que se da una situación de conexidad contractual donde los intervinientes asumen una garantía solidaria. …*" (Cámara de Apelaciones en lo Civil y Comercial, Córdoba, «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)», 29/12/2016, La Ley, AR/JUR/97601/2016).

Otro ejemplo de prácticas llevadas adelante por los proveedores relacionadas a intermediarios de internet/plataformas de comercio electrónico es la utilización de metatags, es decir, búsquedas (a través de buscadores-intermediarios) que lleven a sitios que no guardan estrecha relación con lo buscado y pueden llevar a equívocos al consumidor, constituyendo un supuesto de publicidad engañosa (art. 1101 a) del CCyC), pasible de la acción de cesación del art. 1102. Al mismo tiempo, esto podría ser considerado un uso indebido y no autorizado del nombre o marca.

En nuestro país ha habido un análisis histórico bastante amplio en lo relativo al debate de la responsabilidad de los intermediarios, y la jurisprudencia ha oscilado en torno a su criterio, por lo que la misma no resulta uniforme a la fecha y es uniformemente variada.

En lo que respecta a uno de los proyectos regulatorios específicos que en la materia ha tenido tratamiento, no siendo exento de debate y controversia y que ha perdido a la fecha estado parlamentario, ha sido el proyecto conocido genéricamente por el apellido de su autor: la "Ley Pinedo".

El primer texto de este proyecto contemplaba el detalle que, ante cualquier contenido "cuestionado", el ISP (no se hablaba de intermediarios aún), debía bloquear el contenido.

Luego, al debatirse esto en consonancia con la valoración principiológica que a nivel latinoamericano depositamos en la libertad de expresión, la libre circulación de las ideas y la prohibición de la censura previa, se vislumbró que ello representaba un peligro para estos valores democráticos.

Esto motivó que se comenzaran a denominar "Intermediarios", categoría jurídica donde incluían a distintos sitios donde los usuarios compartían archivos con contenido protegido por derechos de autor (Ej. el antiguo Taringa, que hoy es muy similar a identi.li). Al no estar definido qué era el "contenido cuestionable", pero sí necesitarse una orden judicial para que este sea bloqueado o dado de baja, ello representó un avance en la redacción.

No obstante lo cual, siendo controversial la inclusión dentro de la definición de intermediarios la categoría de intermediario comercial (categoría que debía estar alcanzada por el estatuto consumeril, el que recepta conforme se enunciara previamente, un sistema de responsabilidad objetivo en contradicción con el dispuesto por el proyecto), y no poniéndose de acuerdo en su debate en la definición adecuada del concepto "contenido cuestionable, dicho proyecto perdió estado parlamentario y su debate fue abandonado a la fecha.

Con el fallo de nuestra Corte Suprema de Justicia "R., M. B. v. Google y Yahoo", se estableció en materia de contenidos que el factor de atribución de la responsabilidad elegido a nivel general sería el de la responsabilidad subjetiva, lo que fijó un estándar en materia de responsabilidad de intermediarios por contenidos en internet.

En términos generales, y en todas partes y regiones del mundo, se ha reconocido que los buscadores no tienen una obligación general de supervisión de todos los contenidos subidos a internet, y es por esta misma postura e idea basal que la tesis subjetivista ha sido la que primó jurisprudencialmente en materia de responsabilidad de los buscadores. La inexistencia de la obligación genérica de vigilar los contenidos online ha sido reconocida por organismos internacionales, tales como la ONU y el TJUE para Europa, así como en países de nuestro continente. En nuestro país, conforme al célebre y resonante pronunciamiento de la CSJ argentina en el fallo "R., M. B. v. Google y Yahoo", la balanza se inclinó por esta misma postura y en la distinción de aquellos casos de manifiesta ilicitud en los que el intermediario debiera actuar en pos de la supresión de un contenido de ese tipo.[27]

Esta interpretación y opinión mayoritaria de la Corte no ha estado exenta de discusión tampoco, ya que en la doctrina especialistas han sostenido y señalado la peligrosidad que reviste la interpretación privada y excesiva de aquello considerado como manifiestamente ilícito.

El temor de esta interpretación laxa y de los conceptos jurídicos indeterminados utilizados podría llegar a afectar contenidos que no merecen ser removidos, sustraídos defensivamente de la web, para evitar la aborrecida litigiosidad que los daños producto de los mismos podrían traerle a un intermediario si un potencial afectado reclamase.

---

27 *Véase,* Télam: "Derecho al Olvido". 17.07.2014 13:03hs Internet "Bing también comenzó a adaptarse al derecho al olvido"; 11.07.2014 15:10hs Internet "Google anunció la creación de un consejo de expertos para tratar el "derecho al olvido""; 17.06.2014 19:19hs tendencias "Creo que no hay transparencia, hay censura"; 09.06.2014 16:11hs Internet "Los resultados de Google mostrarían cuando un enlace fue borrado por el "derecho al olvido""; 01.06.2014 10:04hs "La lobotomía de internet"; 30.05.2014 14:59hs Internet "Google presentó una herramienta para ajustarse al "derecho al olvido"" 29.05.2014 14:39hs Internet "Google: "Estamos muy contentos con la decisión de la Corte Suprema de convocar a esta audiencia pública""; 29.05.2014 13:43hs Internet "Concluyó la audiencia pública en la Corte por la responsabilidad de los buscadores de Internet"; 29.05.2014 12:44hs Cultura Digital "La Corte Suprema reanudó la audiencia pública sobre la responsabilidad de los buscadores"; 21.05.2014 10:51hs Internet "Realizaron una audiencia pública en la Corte Suprema de Justicia por la responsabilidad de los buscadores". Link: http://www.telam.com.ar/tags/4349-derecho-al-olvido/noticias

Desde el pronunciamiento en dicho fallo, se han establecido cuáles son algunos de los contenidos que estos intermediarios pueden dar de baja de forma pronta, sin requerimiento de autoridad judicial, sin perjuicio que para los restantes esta sea requerida. En este fallo no se establece qué significa específicamente "notificación fehaciente" más allá que se adopte un criterio subjetivo colaborativo, en similitud con el sistema de "*notice and take down*", con lo cual para muchos el envío de una simple carta documento, implicaría la conservación de evidencia para ese intermediario, a la luz de una causa judicial próxima a iniciarse.

De forma posterior, se ha intentado también a nivel local la modificación de la Ley "Antidiscriminatoria", donde los sectores más vulnerables iniciaron un proyecto de ley para que la discriminación y la violencia que se estaba produciendo en Internet, tuviera una "sanción" más fuerte y estricta.

El principal problema que presentó ese proyecto, en lo particular, fue que las tipificaciones realizadas eran abiertas y no taxativas, contrarias por lo tanto a la Opinión Consultiva N°5 de la CIDH, con lo cual se desistió en el intento de modificación de la ley mencionada.

En la actualidad en la Argentina, se derogó de forma parcial la ley que regulaba a los ISP, la ya mencionada Ley Argentina Digital, que, si bien quedaron vigentes sus ambos artículos sobre neutralidad de la red, el ente regulador no opera eficazmente y no ejerce ningún control efectivo sobre los operadores que brindan distintos tipos de servicios.

En consonancia con esta falencia regulatoria, se prometió la búsqueda de una ley superadora que brinde la unión entre la ley de medios audiovisuales y la ley Argentina Digital, que comenzó por medio del debate de los Principios de Convergencia Digital, lo que fue abandonado a la fecha.

Las responsabilidades por contenidos ilícitos de los intermediarios en estos momentos no es una realidad normativa uniforme. Si bien ha habido fallos de primera instancia donde se condenaba a los intermediarios a pagar una indemnización, luego estos fueron revocados en instancias superiores, hasta llegar al mencionado fallo "R., M. B. v. Google y Yahoo" que sentó opinión en la materia.

En líneas resumidas, la legislación en esta materia aún se encuentra en proceso de debate y tanto las audiencias públicas y encuentros en esta temática, como así los debates en el Congreso de la Nación, han tornado evidente la necesidad imperiosa de una regulación en la materia, no solo en lo civil sino en los distintos códigos de procedimiento penal, ya que a la fecha estos hechos no son reprochables aún desde la tipología penal disponible.

La responsabilidad de los intermediarios al operar con herramientas de privacidad y anonimato, como Tor, redes privadas virtuales / VPN, proxies, entre otras, tal como hemos visto en este desarrollo, depende a nivel local del estatuto que aplique a la misma.

Es decir, si en ella el dañado resulta ser un usuario o un consumidor, el régimen de responsabilidad será el objetivo, que dispone la Ley 24240, y podría ser aplicable el sistema de sanciones administrativas propias de la norma citada, que prescribe en lo específico: *"Art. 47. — Sanciones. Verificada la existencia de la infracción, quienes la hayan cometido serán pasibles de las siguientes sanciones, las que se podrán aplicar independiente o conjuntamente, según resulte de las circunstancias del caso:*

a) Apercibimiento.

b) Multa de PESOS CIEN ($ 100) a PESOS CINCO MILLONES ($ 5.000.000).

c) Decomiso de las mercaderías y productos objeto de la infracción.

d) Clausura del establecimiento o suspensión del servicio afectado por un plazo de hasta TREINTA (30) días.

e) Suspensión de hasta CINCO (5) años en los registros de proveedores que posibilitan contratar con el Estado.

f) La pérdida de concesiones, privilegios, regímenes impositivos o crediticios especiales de que gozare.

En todos los casos, el infractor publicará o la autoridad de aplicación podrá publicar a costa del infractor, conforme el criterio por ésta indicado, la resolución condenatoria o una síntesis de los hechos que la originaron, el tipo de infracción cometida y la sanción aplicada, en un diario de gran circulación en el lugar donde aquélla se cometió y que la autoridad de aplicación indique. En caso que el infractor desarrolle la actividad por la que fue sancionado en más de una jurisdicción, la autoridad de aplicación podrá ordenar que la publicación se realice en un diario de gran circulación en el país y en uno de cada jurisdicción donde aquél actuare. Cuando la pena aplicada fuere de apercibimiento, la autoridad de aplicación podrá dispensar su publicación.

El CINCUENTA POR CIENTO (50%) del monto percibido en concepto de multas y otras penalidades impuestas por la autoridad de aplicación conforme el presente artículo será asignado a un fondo especial destinado a cumplir con los fines del Capítulo XVI —EDUCACION AL CONSUMIDOR— de la presente ley y demás actividades que se realicen para la ejecución de políticas de consumo, conforme lo previsto en el artículo 43, inciso a) de la misma. El fondo será administrado por la autoridad nacional de aplicación." (Artículo sustituido por art. 21 de la Ley N° 26.361 B.O. 7/4/2008)

De otro modo, y frente a otros tipos de relaciones jurídicas donde no intervengan consumidores, por ejemplo, responsabilidad de intermediarios por contenidos, el factor atributivo de la responsabilidad será el subjetivo. Tanto las sanciones, así como los eximentes, son los tradicionales que se corresponden con cada sistema de responsabilidad, lo que no varía teóricamente con los sistemas de responsabilidad que se manejan a nivel regional y del derecho continental.

Finalmente, cabe destacar que, a la fecha en nuestro país, el único fallo que versó indirectamente en materia de utilización de nodos de salida de Tor, por la persecución de un potencial ilícito penal (el de producción de pornografía infantil), ha sido el precedente penal de "Iván Barrera Oro", previamente citado.

Por lo que, en Argentina, no ha habido pronunciamientos aún en el fuero civil y comercial al respecto, específicos en torno a la utilización de herramientas de privacidad y anonimato, su responsabilidad en materia de daños, y las sanciones aplicables a esta tipología particular de casos.

VI. La responsabilidad de los intermediarios al operar con herramientas de privacidad y anonimato por violaciones a la propiedad intelectual

Como en la Argentina la neutralidad de la red se encuentra tipificada en la Ley 27078[28] (denominada y conocida por la Ley "Argentina Digital"), en sus artículos 56 y 57[29] la obligación de los intermediarios a no dar preferencia o depreciar contenido hace que las violaciones a la propiedad intelectual sean tratadas como si no se utilizaran herramientas de privacidad o anonimato.

La responsabilidad civil en las telecomunicaciones ante hechos de terceros resulta nula, y si bien la Ley de Protección de Derechos de Autor 11723 contiene un artículo que remite al Código Penal[30], en referencia a los delitos de Estafa, el fallo de Cámara Nacional de Apelaciones en lo Criminal y Correccional (Sala 4) en el caso "B. M, A y otros s/ Estafa" (Expediente 15161/2012) nos ha dado al respecto la contundente sentencia que enuncia: *"...los tipos penales contemplados en la ley 11.723 no exigen para su configuración un efectivo detrimento patrimonial. Ello, en tanto carecen de las notas típicas de la estafa o la defraudación, debiéndose analizar la cuestión exclusivamente en torno a la afectación de los derechos que el autor -o bien sus causahabientes-, tienen sobre la obra, conforme las previsiones del artículo 5 de la citada ley..."*[31]

Con lo cual, la ya vetusta Ley de Derechos de Autor de la República Argentina, debería ser reformada y acondicionada a los tiempos que corren. Sabemos que las distintas entidades que "protegen", paradójicamente, los intereses de los artistas, son consecuentes con los grandes empresarios que explotan a dichos artistas. Como para nuestra normativa la producción de software es considerada análogamente a la producción de un libro, caemos en cuenta que las distintas reformas planteadas en reiteradas oportunidades por distintos sectores políticos en el Congreso de la Nación se enfrentan ante una barrera muy importante, a saber: el manejo del software por parte de los monopolios, abuso de posición dominante, y la creación de conglomerados de empresas que realizan un "control legal" sobre ciudadanos y pequeñas y medianas empresas.

Son estas últimas, las que, ante la imposibilidad de adquirir el software legal (o ante el desconocimiento) del ciudadano, proceden a propulsar multas de abultada cuantía dineraria, lo que en la práctica se materializa por medio de la solicitud de una reparación integral por el daño ocasionado por la violación de licencias de software.

---

28 Disponible en: http://servicios.infoleg.gob.ar/infolegInternet/anexos/235000-239999/239771/norma.htm

29 ARTÍCULO 56. — Neutralidad de red. Se garantiza a cada usuario el derecho a acceder, utilizar, enviar, recibir u ofrecer cualquier contenido, aplicación, servicio o protocolo a través de Internet sin ningún tipo de restricción, discriminación, distinción, bloqueo, interferencia, entorpecimiento o degradación.
ARTÍCULO 57. — Neutralidad de red. Prohibiciones. Los prestadores de Servicios de TIC no podrán: a) Bloquear, interferir, discriminar, entorpecer, degradar o restringir la utilización, envío, recepción, ofrecimiento o acceso a cualquier contenido, aplicación, servicio o protocolo salvo orden judicial o expresa solicitud del usuario.
b) Fijar el precio de acceso a Internet en virtud de los contenidos, servicios, protocolos o aplicaciones que vayan a ser utilizados u ofrecidos a través de los respectivos contratos.
c) Limitar arbitrariamente el derecho de un usuario a utilizar cualquier hardware o software para acceder a Internet, siempre que los mismos no dañen o perjudiquen la red.

30 Art. 71. - Será reprimido con la pena establecida por el artículo 172 del Código Penal, el que de cualquier manera y en cualquier forma defraude los derechos de propiedad intelectual que reconoce esta ley.

31 Disponible en: https://abogadopoblete.blogspot.com/2016/05/art-71-ley-11723-defraudacion-propiedad-intelectual.html

Ese conglomerado se denomina Software Legal[32] y mantiene una cantidad de empresas en sus filas, tales como Microsoft, Panda, AVG, entre otras, además de mantener un centro de denuncias, y en lo referente a la defensa de sus intereses jurídicos, al estudio BPCM Abogados[33] para litigar e investigar este tipo de acciones.

Claro está que la utilización de herramientas de privacidad e intimidad entorpecería su accionar y no podrían ser funcionales sus investigaciones y litigios judiciales, dado que para ellos deberían poder violentar dichas herramientas. Éstas fomentan la industria al permitir que los usuarios no se vean prisioneros de un proceso monopólico de producción, donde su interacción con la informática es únicamente mediante una determinada empresa, y que, al no poder cumplir con el pago exorbitante que emerge de las distintas "sanciones" por utilizar software copiado, se vean forzados y arrastrados al cierre de sus establecimientos, o simplemente, en la vía constante de precarización del conocimiento y la cultura a la que se encuentran sometidos.

Es por ello que, a nivel nacional, las herramientas de privacidad y anonimato sirven efectivamente como una barrera técnica natural de defensa frente a los abusos que evidencia palmariamente la industria moderna en materia de propiedad intelectual, respecto de la libre circulación del conocimiento y la cultura.

VII. Monitoreo de datos, tráfico de nodo de salida por parte de autoridades. Orden judicial.

Corría el año 2004 en Argentina y la oleada de secuestros de personas hacía inevitable tomar medidas en materia de seguridad física a nivel ciudadanía. Entre las que se tomaron, algunas de ellas resultaron desesperadas por parte del gobierno de ese entonces, el que se enfrentaba a la transición económico y política que aquejaba al país desde el año 2001, donde hubo una notoria crisis financiera y bancaria que tuvo repercusión y trascendencia pública internacional.

El entonces presidente, Néstor Kirchner, firmó para ello el Decreto Presidencial 1563/04[34] que reglamentaba la Ley 25873[35] conocida como la Ley de Telecomunicaciones.

El citado Decreto reglamentó la conservación por parte de los intermediarios (conocidos en ese entonces como "titulares de la licencia de servicio"), por un lapso de 10 (diez) años, tal cual lo definía el artículo 3° inc d), el que enunció: *"Los licenciatarios de servicios de telecomunicaciones deberán conservar los datos filiatorios de sus clientes y los registros originales correspondientes a la demás información asociada a las telecomunicaciones, por el término de DIEZ (10) años..."*.

La acción interpuesta por el Dr. Halabi, al respecto de ello, conocido como el *leading case* del Fallo Halabi, fue la primera acción de clase en su tipo, interpuesta en nuestro país. El objeto de la misma versaba en torno a la privacidad de las comunicaciones entre un abogado y su cliente, respecto de la cual debía hacerse prevalecer el principio de confidencialidad y reser-

---

32 Disponible en: http://www.softwarelegal.org.ar/

33 Disponible en: http://www.bpcm.com.ar/

34 Disponible en: http://servicios.infoleg.gob.ar/infolegInternet/anexos/100000-104999/100806/norma.htm

35 Disponible en: http://servicios.infoleg.gob.ar/infolegInternet/anexos/90000-94999/92549/norma.htm

va, conocido en la doctrina extranjera como el privilegio abogado-cliente.

El motivo por el cual no se deberían almacenar estas comunicaciones, se desprende de manera directa de la privacidad y la protección de los datos personales del cliente, y del deber y obligación de guardar confidencialidad y reserva que pesa sobre el profesional.

A modo de cronología, en el transcurso de la mitad del proceso (y cuando fácticamente el peligro de los secuestros de personas disminuyó y mejoró relativamente la seguridad a nivel local), el mismo presidente Néstor Kirchner emitió un nuevo decreto, el Decreto 557/05.

Este Decreto procedió a eliminar esta captura de las telecomunicaciones, sin perjuicio de que el caso Halabi llegó hasta instancias de la Corte Suprema de Justicia de la Nación, donde quedó establecida la diferencia entre "datos de contenido" y "datos de tráfico".

Se estableció, a su vez, la necesidad de solicitar los datos de tráfico mediante orden judicial de autoridad judicial competente, lo que paradójicamente, rara vez se realiza en los procesos en la Ciudad Autónoma de Buenos Aires, donde se omite lo nombrado por prácticas e informalismos procesales del propio Ministerio Publico Fiscal de la Ciudad Autónoma de Buenos Aires[36].

En lo que respecta a la obtención de datos de contenido, la misma debe siempre efectuarse a pedido de Fiscal y con orden de un Juez[37] y por un tiempo determinado, no mayor a 45 días en el caso de la Ciudad Autónoma de Buenos Aires.

Es por ello que solo queda vigente la interceptación de comunicaciones por este plazo de tiempo, y los intermediarios no solo no tienen ninguna obligación de mantener a resguardo comunicaciones completas (datos de contenido), sino que los datos de conexión (datos de tráfico) solo pueden ser utilizados para demostrar que el servicio funciona de forma correcta a la luz de la Ley de Defensa del Consumidor[38], o para garantir el vital funcionamiento de las telecomunicaciones, tal como como establece la citada Ley Argentina Digital.

Todas las interceptaciones restantes realizadas se efectúan por fuera de la ley, y su obtención no puede ser válida en el marco de un proceso judicial, por la denominada "Teoría del fruto del árbol envenenado".[39]

Claramente, en consonancia con ello y lo restrictivo de esta materia, es que se quiere e impulsa la idea de reformar el Código Procesal Penal de la Nación Argentina. Todo ello con el fin de instrumentar el allanamiento a distancia, la introducción de software malicioso, incluir GPS en las investigaciones, la obligación de los intermediarios a prestar colaboración en la investigación de delitos y la responsabilidad penal correlativa al negarse a ello.

La introducción de estos cambios en el código de forma, permitiría la realización de acciones repudiables desde el punto de vista de la privacidad, anonimato, confidencialidad, y

---

36 Disponible en: https://www.mpf.gob.ar/protex/files/2013/11/Intervencion_Telefonica.pdf

37 Art 93 CPPCABS.

38 Ley 24.240.

39 Disponible en: http://www.saij.gob.ar/maria-victoria-cavagnaro-prueba-ilegal-proceso-penal-alcances-doctrina-fruto-arbol-veneno-so-dacj050082-2005/123456789-0abc-defg2800-50jcanirtcod La prueba ilegal en el proceso penal: alcances de la doctrina del fruto del árbol venenoso por MARÍA VICTORIA CAVAGNARO, ANA PAULA CELIZ. 2005 www.saij.jus.gov.ar Id SAIJ: DACJ050082

protección de datos, entre otros derechos de la ciudadanía, bajo el amparo de la autorización ampliada de perseguir la ciberdelincuencia.

Esta temática fue tratada en el transcurso del presente año, en el Congreso de la Nación Argentina, donde los Senadores dieron media sanción a la norma que modifica el Código Procesal Penal Argentino, con la salvedad que retiraron el artículo que incluía este tipo de interceptaciones.

Más allá de su resultado, el artículo fue retirado no porque los Senadores legislaran para la sociedad en conjunto, sino que se vislumbraron sus peligros a todo nivel y se evidenció que estos métodos investigativos podían ser utilizadas para que el Poder Judicial afín al gobierno de turno, investigue a la oposición parlamentaria en detrimento de esta.[40]

El monitoreo de Tor Exit Nodes en Argentina solo puede efectuarse bajo orden judicial de autoridad competente, como máximo por el plazo de 45 días, y si no es realizado de forma correcta, carece absolutamente de validez y eficacia legal, y su obtención fuera de estos parámetros de licitud conlleva a la realización para ello de nada más que un delito.

VIII. Evidencia digital en materia penal. Incautación de servidores de Tor relays. Admisibilidad. Utilización de Tor para recolectar evidencia. Validez. Validez del agente anonimizado.

Para el proceso penal, donde el allanamiento y el retiro de equipos es la regla para la investigación judicial de delitos informáticos, nos encontramos ante un inconveniente de peso a la hora de hablar de Tor Exit Nodes.

Cuando se comete algún hecho ilícito mediante la utilización de Tor Exit Nodes, luego de la causa contra Iván Barrera Oro y las distintas presentaciones efectuadas en consecuencia en eventos de seguridad informática, el propio Ministerio Publico Fiscal de la Ciudad Autónoma de Buenos Aires nos consultó específicamente respecto de cuál era la forma apropiada de investigar a los distintos tipos de Relays.

Resulta claro que las denuncias llegan por NCMEC[41], donde los distintos sitios webs reportan los delitos contra la integridad sexual de menores y ésta los deriva a las distintas fuerzas de seguridad, según el origen de las direcciones IP para su análisis e investigación judicial en caso de ser necesario. Esto es lo que regularmente sucede con las denuncias de origen extranjero.

Respecto de las denuncias de origen local, nunca son sobre algún Relay en el extranjero. Por el contrario se dejan habitualmente de lado en la investigación judicial, tal como sucedió en la causa judicial que versó sobre las vulnerabilidades encontradas en el sistema de voto electrónico en la Ciudad Autónoma de Buenos Aires en el año 2015, que tuvo como imputado a Joaquín Sorianello[42], donde además del suyo, existieron 5 ingresos "denunciados" de los cuales 2 fueron realizados mediante Tor Exit Nodes desde USA, más precisamente desde las IP 209.222.8.196 y 23.253.21.156.

---

40 Disponible en: https://www.cronista.com/economiapolitica/En-una-sesion-tensa-el-Senado-aprobo-cambios-al-Codigo-Procesal-Penal-20180426-0046.html

41 Disponible en: http://www.missingkids.org/

42 Disponible en: http://www.politicargentina.com/notas/201608/16044-voto-caba-2015.html

Es aquí donde debemos hacer un alto en el camino y recordar que, en el año 2016, año en el que fue realizada la investigación judicial, Argentina no integraba aún el Convenio de Budapest sobre Cibercrimen, y que, de haberlo integrado en su entonces, se podría haber solicitado la colaboración a los Estados Unidos para la investigación de ambos Tor Exit Nodes.

Es por ello, dada la trascendencia del Convenio de Budapest, que las distintas organizaciones de la sociedad civil y la vasta mayoría de los abogados especialistas en esta problemática, nos encontramos consternados por la reunión de Octopus[43] que se llevará a cabo del 9 al 13 de julio en Francia, la que claramente es motivada para un segundo protocolo, al ver que los Estados Unidos se encuentran modificando su propia normativa interna, por medio de la resonante y más reciente CLOUD ACT. Es por todo ello que se motiva el llamado urgente a la reunión de Octopus.

En lo que respecta a nuestro país específicamente, Argentina ingresó formalmente al Convenio de Budapest en el año 2017, al cual adhirió con algunas reservas.

Ahora bien, dicho todo ello, el principal problema reside cuando contamos con empresas, organizaciones de la sociedad civil o personas físicas con sus equipos y su conexión a Internet como Tor Exit Nodes.

Desde el año 2008 los delitos informáticos se encuentran tipificados en el ordenamiento penal. Todos nuestros delitos informáticos son delitos "dolosos", es decir que la mera "culpa" no hace punible el hecho, sino que requiere si o si de la intención de cometer la acción típica, antijurídica y culpable.

Con lo cual y dicho lo que antecedió, en la letra del Código Penal se encuentran excluidos los Tor Exit Nodes, porque no media responsabilidad penal alguna al no existir una regla que diferencie, distinga ni tipifique quién utiliza Tor para cometer hechos ilícitos, de quien los utiliza para mantener y preservar su privacidad e intimidad, o para poder expresar su palabra e incluso poder trabajar (como es el caso de la libertad de expresión, que se encuentra garantizada a su vez en tratados de derechos humanos con jerarquía constitucional en la Argentina que fueron incorporados a nuestro bloque constitucional en el año 1994 en el Art. 75 Inc. 22).

El problema reside en los defectos de la investigación judicial y la falta de capacitación de las distintas fuerzas en el funcionamiento de la red TOR, y en que la responsabilidad de los actores que intervienen en ello resulta nula, todo lo cual genera gastos económicos enormes para nuestro país.

Estas fallas de eficacia y eficiencia forense en la materia, consume recursos vitales en la investigación judicial de delitos informáticos e infraestructura legal. Nuestros tribunales actualmente se encuentran colapsados y sumar expedientes que no tienen asidero legal por ausencia de protocolos forenses adecuados carece de todo sentido pragmático, dado que, los presuntos autores de los ilícitos, luego de ser allanados injustamente, son quienes luego reclaman al propio Estado la reparación de los daños y perjuicios ocasionados por la propia ignorancia o incapacidad de las fuerzas de seguridad en identificar que las direcciones IP

---

43 Disponible en: https://www.coe.int/en/web/cybercrime/octopus-conference

brindadas por NCMEC que son Tor Exit Nodes, y por haber sido injustamente traídos a un proceso del que no se termina por corroborar ningún hecho por imposibilidad fáctica.

Si bien, para la práctica forense puede resultarle extraño, no todas las fuerzas en investigación saben utilizar servicios tales como Exonerator[44], que no solo permite que el Estado ahorre dinero, sino que sirve como control judicial eficiente y como mecanismo para mantener recursos apropiados para el análisis del delito.

Por último, la figura del agente encubierto y el agente revelador (como provocador) se encuentra regulado en Argentina desde el año 2016 por la Ley 27319[45]. Esta figura está reglada para ciertos delitos complejos, y su investigación en relación a los delitos informáticos se centra en el artículo 128 del Código Penal, por el cual se condena la pornografía infantil[46].

Mas allá que para la persecución de los delitos de narcotráfico y trata de personas en los que se suelen utilizar distintas formas de investigación complementarias casi siempre la figura se encuentra presente, la misma no referencia a ninguna utilización específica de sistemas informáticos para la investigación de delitos, sean o no mediante Tor o cualquier otro sistema. Sin embargo, si establece que debe ser informado al Juez de inmediato, con lo cual estas investigaciones se realizan siempre por tiempo determinado y bajo estricto control judicial.

La prueba obtenida bajo un agente encubierto puede ser realizada bajo la utilización de Tor bajo las condiciones de un proceso judicial que lo solicite, pero no hay razón legal alguna en la que el Estado Nacional Argentino coloque un Exit Tor Nodes para controlar tráfico, analizar o conservar datos para utilizar en un futuro, dado que las condiciones para interceptar comunicaciones som únicamente posiblse en cumplimiento estricto de un marco de tiempo muy reducido (45 días máximo en la Ciudad Autónoma de Buenos Aires), y los plazos para la investigación judicial en la etapa de instrucción son también acotados.

Es por todo ello, que resta añadir que la reciente intención de modificar el Código Procesal Penal de la Nación en el año 2018, para incluir como metodología en las investigaciones especiales, los allanamientos a distancia, utilización de GPS, malware, etc., no llegaron a buen puerto y se encuentran sin progreso. La utilización de estas técnicas como método de investigación y persecución cibercriminal fue ampliamente combatido tanto por las organizaciones de la sociedad civil en defensa de los derechos y garantías constitucionales de los individuos, así como por una vastedad de referentes jurídicos en la materia.

---

44 Disponible en: https://exonerator.torproject.org/

45 Disponible en: http://servicios.infoleg.gob.ar/infolegInternet/anexos/265000-269999/268004/norma.htm

46 ARTICULO 128 — Será reprimido con prisión de tres (3) a seis (6) años el que produjere, financiare, ofreciere, comerciare, publicare, facilitare, divulgare o distribuyere, por cualquier medio, toda representación de un menor de dieciocho (18) años dedicado a actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales, al igual que el que organizare espectáculos en vivo de representaciones sexuales explícitas en que participaren dichos menores.
Será reprimido con prisión de cuatro (4) meses a un (1) año el que a sabiendas tuviere en su poder representaciones de las descriptas en el párrafo anterior.
Será reprimido con prisión de seis (6) meses a dos (2) años el que tuviere en su poder representaciones de las descriptas en el primer párrafo con fines inequívocos de distribución o comercialización.
Será reprimido con prisión de un (1) mes a tres (3) años el que facilitare el acceso a espectáculos pornográficos o suministrare material pornográfico a menores de catorce (14) años.
Todas las escalas penales previstas en este artículo se elevarán en un tercio en su mínimo y en su máximo cuando la víctima fuere menor de trece (13) años.

Conclusiones

El reconocimiento constitucional y legal extendido en Argentina respecto de los derechos a la intimidad, privacidad, protección de datos, autodeterminación informativa, confidencialidad, reserva, entre otros, permite reflexionar respecto de la utilidad que representan las herramientas de privacidad y anonimato, tales como Tor, respecto de la defensa de estos derechos y el empoderamiento ciudadano a través de su ejercicio práctico.

La ausencia de una prohibición legal específica, así como la ausencia de tipificación penal respecto de la utilización de técnicas de anonimato, privacidad, seudonimia o cifrado, derivan en razonable, legal y permitida la utilización de herramientas de privacidad y anonimato en Argentina.

La utilización de herramientas de privacidad y anonimato, tales como Tor, permiten el robustecimiento y empoderamiento ciudadano a través de su contribución a la libre circulación de las ideas, libertad de expresión y como metodología que permite evitar pragmáticamente las maniobras de censura previa que atentan contra estos derechos garantizados a nivel constitucional y por tratados humanos de máximo rango y jerarquía a nivel regional e internacional.

Resulta una práctica generalizada y en franco crecimiento, tanto en entornos de privacidad, por necesidad operativa, como por aquellos usuarios consientes y rigurosos respecto de su privacidad, el recurrir a la utilización de herramientas de privacidad y anonimato, tales como Tor, las que se encuentran legalmente permitidas por nuestro sistema jurídico.

Las tesis utilizadas en materia de imputación de la responsabilidad de los intermediarios de internet, a saber, la de responsabilidad subjetiva, objetiva y la tesis de la irresponsabilidad, resultan el matiz de respuestas disponibles jurisprudenciales en los casos en los que se disputa el factor de atribución aplicable.

En todos aquellos entornos, así sea en aquellos donde se utilizan herramientas de privacidad y anonimato, en los que intervenga un consumidor como parte, por ley a nivel local, debe aplicarse en materia de atribución de la responsabilidad el factor objetivo, que prescinde del dolo o la culpa del agente dañador. Mientras que, por otra parte, en aquellos casos en los que se encuentra primordialmente en juego bienes jurídicos y derechos tales como la libertad de expresión, la tesis sostenida mayoritariamente a nivel judicial local ha sido la de la responsabilidad subjetiva.

Se concluye como necesaria la adopción de mecanismos y criterios uniformes en materia de responsabilidad civil en torno a los daños potencialmente ocasionados, por vía de la utilización de herramientas de privacidad y anonimato, ya que los criterios de responsabilidad por daños que se manejan actualmente en la materia, no sólo no resultan homogéneos, hasta en ocasiones antagónicos, sino que más gravosamente, no responden a los contextos tecnológicos que plantean estas herramientas.

Las herramientas de privacidad y anonimato también sirven efectivamente como una barrera técnica natural de defensa frente a los abusos característicos de la industria moderna privativa empresarial en materia de propiedad intelectual, respecto de la libre circulación del conocimiento y la cultura, y lo que ello significa para la educación y capacitación de las personas, como derechos humanos fundamentales.

En lo que respecta a la investigación forense pasible a realizar en esta tipología de herramientas, a nivel local, el monitoreo de Tor Exit Nodes solo puede efectuarse sujeto a orden judicial de autoridad competente, como máximo por el plazo de 45 días, mientras que, por el contrario, su obtención fuera de estos parámetros deviene ilícita. Asimismo, la prueba obtenida bajo la figura de un agente encubierto anonimizado puede ser realizada bajo la utilización de Tor bajo las condiciones de legalidad descriptas, dentro un proceso judicial que lo solicite particularmente.

Es necesario optimizar las técnicas, prácticas y protocolos forenses, así como la capacitación, educación y formación continua y de calidad respecto de las características, funcionamiento e implicancias derivadas de la utilización de herramientas de privacidad y anonimato, tales como Tor, puesto que a nivel jurisdiccional se observa de manera generalizada una falta de preparación para la contemplación de casos en los que estas herramientas hayan sido utilizadas. Esto conlleva para la prestación del servicio de justicia fallas de eficacia, eficiencia, así como desperdicio de recursos y daños a particulares afectados por procesos de investigación injustos, que únicamente terminan por vulnerar sus derechos intrínsecos.

Tal como se puede derivar de la lectura del texto de nuestra codificación penal, no existe a la fecha en ella ninguna responsabilidad penal explícita que se derive de la utilización de herramientas de privacidad y anonimato como Tor. Debido a que al no existir una regla que diferencie, distinga ni tipifique quién utiliza Tor para cometer hechos ilícitos de quien los utiliza para mantener y preservar su privacidad e intimidad, o incluso de quien para poder expresar su palabra e incluso poder trabajar, no es posible punir ni tipificar de manera genérica su utilización. Es, por todo ello, que nuestra regulación penal local vigente excluye de responsabilidad a los Tor exit nodes.

Finalmente, resta destacar de manera sintética que, a nivel general, los nodos de Tor intermedios no presentan a nivel nacional problemática legal alguna, en contraposición con la mala reputación que gozan a nivel nacional los nodos de salida, los cuales, si bien no acarrean una responsabilidad civil o penal per se, ni se encuentran prohibidos específicamente, se encuentran sujetos a un mayor escrutinio, peligro en cuanto a su examen y posibilidad de ser investigados judicialmente.


DERECHOSDIGITALES
Derechos Humanos y Tecnología en América Latina