COLECCIÓN INSTITUCIONAL

ERA DIGITAL: DELITO Y PREVENCIÓN

Coordinadora: **Vanesa Y. Ferrazzuolo**

Poder Judicial de la Ciudad de Buenos Aires
Consejo de la Magistratura

JUS BAI RES EDITORIAL

Era digital: delito y prevención

www.editorial.jusbaires.gob.ar
editorial@jusbaires.gob.ar
fb: /editorialjusbaires
Av. Julio A. Roca 534 [C1067ABN]
+5411 4011-1320

Sello Buen Diseño argentino

Ferrazzuolo, Vanesa
Era digital: delito y prevención / Vanesa Ferrazzuolo. - 1a ed . - Ciudad Autónoma de Buenos Aires: Editorial Jusbaires, 2019.
Libro digital, PDF

Archivo Digital: descarga y online
ISBN 978-987-768-110-9

1. Derecho de la Informática. I. Título.
CDD 343.09944

Hecho el depósito previsto según Ley N° 11723

Declarada de interés por la Legislatura de la Ciudad Autónoma de Buenos Aires.
Res. Nro. 543-2018

Editorial Jusbaires
Coordinación General: Alejandra García
Dirección: Gerardo Filippelli
Edición: Francisco Berreta y Daiana Fernández
Corrección: Daniela Donni, Leticia Muñoa, Mariana Palomino y Julieta Richiello
Coordinación de Arte y Diseño: Mariana Pittaluga
Colaboración en ilustración de tapa: Facundo Broto
Maquetación: Esteban J. González

La presente publicación ha sido compuesta con las tipografías *Saira* del tipógrafo argentino Héctor Gatti para la fundidora *Omnibus-Type* y *Alegreya* de la fundidora argentina *Huerta Tipográfica*.

Poder Judicial de la Ciudad de Buenos Aires
Consejo de la Magistratura

Autoridades 2019

Presidente

Alberto Maques

Vicepresidente

Alejandro Fernández

Secretaria

Lidia Ester Lago

Consejeros

Raúl Alfonsín
Silvia Bianco
Vanesa Ferrazzuolo
Anabella Hers Cabral
Darío Reynoso
Marcelo Vázquez

Administrador General

Luis Hernando Montenegro

ÍNDICE

Presentación

Vanesa Y. Ferrazzuolo

En un mundo globalizado, en el que las nuevas tecnologías se convirtieron en una parte esencial de lo cotidiano, esta obra es imprescindible para comprender las implicancias de la irrupción de lo digital en las diversas esferas de interacción social.

En el plano jurídico, destacados operadores del sistema de justicia analizan en profundidad los delitos informáticos y las técnicas incorporadas en la investigación criminal en la era digital.

Precisamente, la diferencia de roles que desempeñan los autores enriquece este trabajo, que aborda los principales debates e interrogantes sobre el delito y las nuevas tecnologías.

Los problemas y desafíos que representan los delitos informáticos y las modalidades de adquisición y gestión de la evidencia digital en el sistema penal llegan al lector a través del prisma de quienes con su labor profesional cotidiana inciden en la temática.

Por otra parte, desde la experiencia de prestigiosas organizaciones no gubernamentales que trabajan en nuestro país se nos invita a repensar las estrategias de abordaje de las nuevas formas de vinculación en el entorno digital, en procura de resguardar la intimidad y conjurar los peligros que estos modos de interacción posibilitan, interpelando especialmente a padres y educadores.

En síntesis, *Era digital: delito y prevención* nos propone un recorrido sumamente interesante sobre la incorporación de las nuevas tecnologías, de la mano de ocho autores provenientes de distintos organismos, y haciendo foco en la intervención que se efectúa desde el sistema penal, en los peligros a los que se encuentran especialmente expuestos las niñas, los niños y los adolescentes, tanto como en la importancia del rol preventivo que deben desempeñar padres y docentes.

La fiscal a cargo del equipo especializado en delitos informáticos Daniela Dupuy hace su aporte a esta obra colectiva planteando los nuevos desafíos en materia de seguridad digital así como los

obstáculos técnicos y jurídicos que atraviesan las investigaciones en entornos digitales.

En "Ciberdelitos. Desafíos para trabajar" se compila información imprescindible sobre ataques de *malware*, fraudes informáticos, pornografía infantil, *grooming* y *revenge porn*, entre otros. También se pone en cuestión la expectativa de privacidad que merecen los dispositivos de almacenamiento informático y se desarrollan las variadas aristas que supone la incorporación de inteligencia artificial al sistema de justicia.

La Defensoría Pública de la Ciudad Autónoma de Buenos Aires está representada por el Dr. Gustavo Eduardo Aboso, quien se desempeña como Defensor ante la Cámara en lo Penal, Contravencional y de Faltas del Poder Judicial de la CABA. En "Técnicas de Investigación y vigilancia electrónica en el proceso penal y el derecho a la privacidad en la moderna sociedad de la información" desarrolla –desde la óptica del derecho penal– los desafíos que representa la extensión cuasi universal de las nuevas tecnologías en la vida cotidiana de las personas.

A partir del análisis de las experiencias en Alemania y España, deja planteadas las bondades y penurias de los nuevos mecanismos de generación de pruebas, la aparición de nuevas modalidades delictivas, la necesidad de actualización y sistematización de los cuerpos normativos procesales penales y las contradicciones entre los derechos de los ciudadanos –especialmente en relación con el derecho a la privacidad– y la utilización de las nuevas herramientas tecnológicas en la labor de administración e impartición de justicia.

En "Estrategias y planteos en casos de delitos informáticos. Desafíos para la Defensa" la Dra. Yanina G. Matas introduce los debates que resuenan en la actualidad sobre criminalidad informática. Luego de reseñar la evolución normativa en el ámbito local y a partir de su experiencia en el Ministerio Público de la Defensa, analiza decisiones jurisdiccionales relevantes en la materia.

Entre los temas que aborda, destaca las diferencias entre evidencias tradicionales y evidencias digitales, y revela la necesidad de generar mecanismos normalizados y específicos que, en términos procesales, permitan el ejercicio del derecho de forma imparcial.

Otro aporte significativo lo realiza el Dr. Eduardo Aníbal Aguayo, quien se desempeña como Prosecretario Letrado en la Defensoría General de la Nación. Su trabajo titulado "Responsabilidad penal de la

inteligencia artificial. Hacia un paradigma de singularidad tecnológica", articula la cuestión de la Inteligencia Artificial y los conflictos que se generan en torno al desarrollo de esta tecnología de punta. Aborda la cuestión en la actualidad y anticipa las posibles complicaciones o contradicciones que pueden surgir en el futuro en relación con los ordenamientos jurídicos.

En este artículo se abordan en paralelo tanto las perspectivas sobre el impacto jurídico como sobre el desarrollo humano en general. Toma como objeto de análisis la aparición de las IA (inteligencias artificiales) y de la robótica, desentrañando las posibles consecuencias que pueden impactar negativamente en el seno de la vida social. En ese sentido, el autor propone principios orientadores para el desarrollo de estas tecnologías, como la responsabilidad jurídica, el tratamiento ético y la seguridad. A la vez que siembra interrogantes en torno a la capacidad del ser humano sobre el control de las IA, en su capacidad cognitiva o de razonamiento aprehensivo.

Yael Bendel –Asesora General Tutelar de la CABA–, ofrece una aproximación a la problemática que plantea el *grooming* desde la perspectiva garantizadora de los derechos de las niñas, niños y adolescentes.

En "La protección de los derechos de niñas, niños y adolescentes frente al delito de *grooming*" nos presenta una retrospectiva histórica sobre la creación de la figura penal, señalando sus puntos de intersección con la evolución del movimiento internacional de derechos humanos de la infancia, que conminó a los Estados a garantizar los derechos de niñas, niños y adolescentes de modo prioritario.

La Dra. Bendel nos advierte:

> La globalización y la masificación en el uso de las nuevas tecnologías propició enormes beneficios, pero también riesgos, ya que antiguas modalidades delictivas mutaron, se adaptaron y encontraron un mayor caudal de "posibles víctimas", así como posibilidades de nuevas formas de engaño y anonimato en las redes.

Con el énfasis puesto en el concepto de corresponsabilidad –entendida como la obligación de los actores gubernamentales y no gubernamentales de implementar acciones de protección de derechos mediante el trabajo articulado, intersectorial y simultáneo–, interpela

a las instituciones y reclama el protagonismo de escuela y familia en la creación de espacios de reflexión sobre el uso de las nuevas tecnologías.

La ONG Faro Digital –colectivo multidisciplinario para la construcción y promoción de la ciudadanía digital– nos ayuda a reflexionar sobre vínculos, relaciones y formas de comunicarse entre las personas, en el contexto de un mundo digital y conectado.

"Internet, un espacio comunicacional y de construcción de diálogo intergeneracional" pone en crisis nuestras propias construcciones de sentido sobre el uso de las tecnologías digitales, como presupuesto necesario para el intercambio de saberes. También brinda herramientas para afrontar la brecha generacional en las formas de aprehensión digital de los adultos, los jóvenes y los niños. Tales herramientas, a su vez, nos permitirán apreciar la verdadera dimensión de los conflictos a los que están expuestos niñas, niños y adolescentes en sus interacciones cotidianas en la *web: ciberbullying*, viralización de imágenes sin consentimiento, *grooming*, violencia digital, construcción de reputación *web* o identidad digital, etcétera.

Con dinamismo y valiéndose de un lenguaje sumamente accesible, Faro Digital pone en el centro de la escena la dinámica entre padres e hijos en relación con la tecnología. Muestra un camino para acompañar adecuadamente los trayectos digitales de los más chicos, promoviendo la consolidación de los progenitores como referentes de cuidado, para contribuir a generar espacios digitales libres de burlas, discriminación, hostigamiento y discursos de odio.

La ONG Argentina Cibersegura también pone el eje en el enfoque preventivo, trazando las coordenadas que vehiculizan el equilibrio entre la generación de herramientas por parte de niños y jóvenes y el resguardo de su seguridad.

Para ello nos sumerge en los problemas que conlleva la utilización de Internet y, desde allí, desanda los presupuestos necesarios para el ejercicio eficiente de la capacidad de cuidado.

Con una visión optimista, "*Grooming*: el desafío para cuidar a los más chicos" provee el andamiaje conceptual imprescindible para que la tecnología colabore en acortar brechas entre grandes y chicos. Herramientas de control parental, mundo físico como fuente de analogías, reglas claras y compromiso compartido, y el ejemplo como base

de la educación son algunas de las premisas que favorecen que se produzca el clima de confianza necesario para minimizar los riesgos.

Uno de los trabajos compilados tiene particular relevancia en tanto fue concebido por el integrante del Consejo de la Magistratura que hizo posible la articulación de las Organizaciones No Gubernamentales especializadas en ciberdelitos con el Poder Judicial de la Ciudad: el Dr. Alejandro Fernández. Su trabajo parte de la dicotomía que genera la masificación de Internet en términos de identidad y anonimato, realidad y virtualidad, publicidad e intimidad, control y publicidad, y libertad y responsabilidad. En definitiva, pone en el tapete la convivencia digital, planteando si la masificación de Internet constituye una nueva herramienta o un nuevo conflicto.

"Internet y las nuevas formas sociales, jurídicas y punitivas" elabora una serie de buenas prácticas para tener en cuenta a la hora de navegar y promover un uso responsable de las redes. Así, se refiere al aseguramiento del anonimato, al resguardo de las comunicaciones privadas, y a la seguridad y el cuidado de los datos personales, entre otras.

También revela los conflictos que se suscitan en relación con derechos fundamentales como el acceso a la información y a la libertad de expresión, y por último describe la evolución de la jurisprudencia nacional sobre los ciberdelitos y su adaptación dinámica al contexto social.

Esta obra colectiva, en definitiva, promueve la reflexión sobre las diversas aristas que introducen las nuevas tecnologías, alertando acerca de sus posibles consecuencias en el siglo XXI, tanto desde el punto de vista jurídico como para la sociedad en su conjunto.

Técnicas de investigación y vigilancia electrónicas en el proceso penal y el derecho a la privacidad en la moderna sociedad de la información

Gustavo Eduardo Aboso*

Introducción

En la actualidad se discute el sentido y alcance de los medios de prueba en materia penal a la luz de la irrupción de las nuevas tecnologías y técnicas de investigación aplicadas, por ejemplo, en la detección e identificación del ADN.[1] Este progreso aparentemente inagotable orientado hacia el mejoramiento de las técnicas de investigación en materia procesal penal trajo aparejada la necesidad de armonizar los textos normativos a esta nueva realidad.

En el caso argentino, las leyes procesales penales no incluyen dispositivos dedicados de manera exclusiva a la regulación de la investigación de la cibercriminalidad, más allá de las normas procesales que autorizan en trazos generales la interceptación de las comunicaciones y el secuestro de correspondencia o papeles privados (arts. 231 y ss. del

* Doctor en Derecho (UNED - Madrid). Defensor de Cámara en lo Penal, Contravencional y de Faltas del Poder Judicial de la Ciudad Autónoma de Buenos Aires. Profesor de grado y posgrado de Derecho Penal (UBA, Universidad Austral y Universidad Nacional de Mar del Plata).

1. Cortés Bechiarelli, Emilio, "El insoportable anacronismo de los abusos policiales en el marco de la instrucción criminal a la luz de las nuevas técnicas de investigación", en González Cussac, José Luis y Cuerda Arnau, María Luisa (dirs.); Fernández Hernández, Antonio (coord.), *Nuevas amenazas a la seguridad nacional. Terrorismo, criminalidad organizada y tecnologías de la información y la comunicación*, Valencia, Tirant Lo Blanch, 2013, p. 47 y ss. En este sentido, el art. 218 *bis* del Código Procesal Penal de la Nación regula la medida de obtención de ácido desoxirribonucleico (ADN) con fines de identificación o para la acreditación del hecho investigado. Al respecto, la medida procesal de extracción de sangre está prevista por el art. 198 del Código Procesal Penal de Córdoba.

Código Procesal Penal de la Nación; arts. 115 y 117 del Código Procesal Penal de la Ciudad Autónoma de Buenos Aires; arts. 214 y 216 del Código Procesal Penal de Córdoba; arts. 208 y 213 del Código Procesal Penal de la provincia de Formosa, entre otros), en los términos previstos por el artículo 18 de la Constitución Nacional.

Al respecto, el nuevo Código Procesal Penal de la Nación (Ley Nº 27063), cuya entrada en vigor para este año ha quedado suspendida (Decreto PEN Nº 257/2015), prevé en su artículo 143 la interceptación de correspondencia electrónica o de cualquier otra forma de comunicación, pues tal intervención será de carácter excepcional y por un plazo máximo de treinta (30) días, término que puede ser prorrogado. Por la importancia de esta medida, solo puede ser autorizada por mandato judicial. El párrafo quinto de este artículo 143 establece el deber de colaboración de los titulares del servicio de comunicación. Al mismo tiempo, el artículo 144 de esta ley establece la facultad del juez de disponer el registro de un sistema informático o de un medio de almacenamiento informático o electrónico, con el objeto de utilizar sus componentes, obtener copia o preservar datos o elementos de interés para la investigación.

En cambio, en el Derecho Comparado es posible vislumbrar una tendencia reformista orientada hacia la armonización de las normas procesales a la complejidad de las infracciones informáticas.[2] El propio Convenio sobre la Ciberdelincuencia de 2001 (STE Nº 185) proyecta un número importante de normas procesales penales en materia de interceptación, registro, conservación, tratamiento y almacenamiento de datos informáticos (arts. 14 a 21), con el propósito de armonizar las legislaciones procesales de naturaleza penal a este fenómeno virtual.

En el Derecho Procesal alemán, por ejemplo, se ha introducido un conjunto de reformas que regulan las investigaciones policiales en materia de terrorismo, crimen organizado y demás delitos graves; en especial, se autoriza a recurrir a distintos métodos de pesquisa, en consonancia con el grado de dificultad probatoria que presentan es-

2. González Cussac, José, L., "Estrategias legales frente a las ciberamenazas", en *Cuadernos de Estrategia*, Nº 149, 2011, p. 85 y ss.; García González, Javier, "Intervenciones de terceros en el correo electrónico. Especial referencia al ámbito laboral y policial", en Romeo Casabona, Carlos María (dir.), *El cibercrimen. Nuevos retos jurídico-penales, nuevas respuestas político-criminales*, Estudios de Derecho Penal y Criminología, Granada, Comares, 2006, p. 314 y ss.

tos delitos y la necesidad de anticipar posibles atentados terroristas, circunstancia que habilita el uso de herramientas técnicas apropiadas para infiltrarse en las computadoras personales de los sospechosos, obtener información sobre actividades terroristas y seguimiento de los integrantes de las organizaciones criminales de esta naturaleza.

Los §§ 94 y siguientes del Código Procesal Penal alemán (*Strafprozeßordnung* o StPO) establecen una serie de medidas probatorias tendientes a la identificación de sospechosos de delitos graves sobre la base del entrecruzamiento de datos informáticos (§ 98a StPO), medidas que están sujetas al control judicial (§ 98b). Entre las (medidas) disposiciones de investigación, se cuentan la interceptación y el registro de correos electrónicos de un sospechoso (§§ 99 y 100a); los que solo pueden ser autorizados por la autoridad judicial hasta un plazo máximo de tres meses (§ 100b). De particular trascendencia resultan las medidas de seguimiento, registro fílmico y fotográfico del presunto autor, así como también la interceptación y registro de las conversaciones privadas mediante el uso de recursos tecnológicos adecuados para esa finalidad (§ 100c). Estas medidas son de carácter excepcional y deben ser homologadas por el juez (§ 100d).

Una regulación análoga en materia de interceptación de comunicaciones telefónicas y telemáticas se encuentra en la Ley de Enjuiciamiento Criminal española. El Capítulo IV del Título VIII, denominado "De las medidas de investigación limitativas de los derechos reconocidos en el artículo 18 de la Constitución", del Libro II de esa ley contiene una serie de artículos que disponen las condiciones de procedencia de esta clase de medidas y su alcance. El artículo 588 *bis* a) enumera los principios rectores en materia de investigación electrónica sujeta al control judicial y tributario de los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad. Conforme a estos principios, está vedado recurrir a esta forma de investigación para prevenir o descubrir delitos o despejar sospechas sin base objetiva. Así pues, se prohíbe la interceptación de comunicaciones telefónicas y telemáticas con el propósito de investigar la eventual comisión de delitos (finalidad preventiva). En todo caso, habrá de requerirse la existencia de una objetiva comprobación material de la comisión de un delito. El principio de idoneidad sirve a los fines de evaluar el sentido y alcance de tal medida de investigación, en cuyo caso el juez que la otorgara

deberá motivarla y determinar el plazo temporal de la duración de esa intervención judicial (art. 588 *bis* c y 588 *bis* e), aunque la ley establece por regla un plazo de tres meses, prorrogables por períodos sucesivos de igual duración, hasta un máximo de dieciocho meses (art. 588 *ter* g). Finalizado el procedimiento y dependiendo de su resultado, el juez deberá ordenar la destrucción de los registros realizados (art. 588 *bis* k).

Como ocurre en el caso alemán, las interceptaciones telefónicas y telemáticas solo son procedentes para cierta clase de delitos, enumerados en el artículo 579.1 de la Ley Procesal Penal,[3] o bien cuando para la realización del delito se hayan utilizado instrumentos informáticos, sea derivados de la tecnología de la información o del servicio de comunicación (art. 588 *ter* a). Como se dijo precedentemente, la autorización judicial es una condición indispensable, salvo en caso de una urgencia originada por la actuación de bandas armadas o elementos terroristas, en cuyo caso tal orden podrá provenir del ministro del Interior o, en su defecto, del secretario de Estado de Seguridad. Esa medida deberá ser comunicada de manera inmediata al juez competente, quien deberá homologarla o revocarla (art. 588 *ter* d).

En particular, la Ley Procesal Penal española regula la incorporación al proceso de datos electrónicos de tráfico o asociados que hayan sido almacenados en función de lo previsto por la propia Ley de Registro o por propia iniciativa de los prestadores del servicio, y será necesaria en todo caso la autorización judicial para su cesión (art. 588 *ter* j). En este último aspecto, cabe decir que, a nuestro criterio, el registro y almacenamiento de datos personales de los usuarios del servicio de Internet ofrecido por la empresa privada deberá estar debidamente justificado, ya que las razones comerciales de su uso no legitima por sí solo su registro o cesión a terceros, máxime cuando entre los datos almacenados se encuentran aquellos que guardan relación de afinidad con los datos personales o sensibles.

El uso extensivo de medios, sistemas de control y vigilancia en la vía pública o en lugares determinados (cámaras de seguridad,

3. El art. 579.1 autoriza la detención judicial de correspondencia privada, postal y telegráfica, incluidos faxes, burofaxes y giros, remitidos o enviados por el investigado, siempre y cuando el objeto del proceso consista en la investigación de delitos dolosos castigados con pena con límite máximo de, por lo menos, tres años de prisión; delitos cometidos en el seno de un grupo u organización criminal; o bien delitos de terrorismo.

drones);[4] la introducción de parámetros biométricos para identificar a las personas; la aplicación de programas informáticos para detectar la ubicación de un individuo o el tratamiento de los datos colectados en una tarjeta inteligente para averiguar los movimientos diarios de los usuarios de un servicio de transporte público o privado; la obtención de datos personales o preferencias de los usuarios de los sistemas informáticos;[5] la geolocalización mediante el empleo de satélites, los dispositivos de búsqueda vehicular y otro tipo de sistema o artefacto que permitan conocer en tiempo real la ubicación de una persona; todo ello ha encontrado un campo fértil para su activa aplicación en el ámbito del Derecho Procesal Penal.

Como es sabido, a partir de los ataques terroristas de septiembre de 2001 se generó un cuadro de paranoia general que determinó la adopción

4. Muñoz Conde, Francisco, *Valoración de las grabaciones audiovisuales en el proceso penal*, Buenos Aires, Hammurabi, 2004, p. 41 y ss., p. 56 y ss. En el ámbito laboral, el uso de sistemas cerrados de videograbación para detectar posibles irregularidades o delitos por parte de los trabajadores ha generado innumerables demandas por despido injustificado sobre la base de la vulneración de la dignidad humana, el derecho a la imagen y la protección de datos, cfr. STCE N° 39/2016, del 3 de marzo. En esta sentencia se afirmó que el consentimiento del trabajador no era necesario porque el tratamiento de las imágenes obtenidas del sistema de videocámaras instalado en la empresa obedeció a la finalidad de seguridad o control laboral, con arreglo a la Ley Laboral. Por lo demás, el uso del sistema de videocámaras guardaba relación de proporcionalidad con la finalidad pretendida. También la STCE N° 29/2013, del 11 de febrero, hace un repaso de la doctrina aplicada por ese tribunal en el caso del uso de videocámaras para controlar el acceso y egreso de profesores de una universidad, siendo utilizadas las videofilmaciones para justificar las sanciones disciplinarias por incumplimiento laboral. La STCE N° 98/2000, en pleno, del 30 de noviembre, se ocupa del ejercicio del control empresarial mediante la instalación de micrófonos en las dependencias laborales con conocimiento de los trabajadores y del Comité de Vigilancia de la empresa. En general, los agravios abarcan la violación a los derechos del honor y de la imagen, pero también la protección de datos personales. Sobre la regulación de los sistemas de videocámaras, Brown, Jeremy, "Pan, Tilt, Zoom: Regulating the Use of Video Surveillance of Public Places", en *Berkeley Technology Law Journal*, Vol. 23, 2008, p. 755 y ss. El uso de sistemas de vigilancia mediante videocámaras –explica este autor– se originó en la ciudad de Mt. Vernon, Nueva York, en 1971 y, posteriormente, se extendió a distintas ciudades americanas, y fue aplicado en la última década a la lucha contra el terrorismo.

5. Geradin, Damien y Kuschewsky, Monika, "Competition Law and Personal Data: Preliminary Thoughts on a Complex Issue", febrero de 2013. Disponible en: http://ssrn.com.abstract=2216088. Explican estos autores que el modelo de negocio empleado por la mayor parte de los proveedores de servicio en Internet presenta dos lados, uno, identificado con la prestación de un servicio gratuito para terceros; el otro, la generación de fondos dinerarios necesarios para sostener este servicio de búsqueda.

de distintas medidas de seguridad, en particular, respecto de medidas contraterroristas, al socaire de la actuación de agencias de seguridad en todo el mundo cuyos presupuestos operativos han sido incrementados de manera exponencial para integrar vastas redes de espionaje informático con el objeto de evitar otros atentados colectivos. Ello derivó necesariamente en una avalancha de medidas de infiltración doméstica y extranjera, incluso de potencias amigas, con el declarado propósito de luchar contra el terrorismo, pero al mismo tiempo con la larvada intención de estrechar el control sobre los gobiernos extranjeros.[6]

En el terreno del derecho a la privacidad, todos nosotros podemos sentirnos controlados o espiados de modo razonable –sin que sea necesario atravesar un estado paranoico– por parte de organismos públicos o privados, ya que una buena parte de nuestros movimientos diarios por las calles, autopistas o en la misma vía pública pueden ser detectados sin mayores inconvenientes en razón de la proliferación de los sistemas de vigilancia audiovisual. Londres ha sido una de las primeras ciudades en recurrir a este tipo de sistema de vigilancia mediante videocámaras (el llamado *London's Ring of Steel*) para reforzar la seguridad pública en sus calles y luego otras ciudades, como Nueva York, se han sumado a esta iniciativa para fijar un ámbito espacial de máxima seguridad contra atentados terroristas (el denominado *Lower Manhattan Security Initiative*).[7] Este tipo de medidas de seguridad mediante la instalación de cámaras se ha extendido hasta abarcar la Ciudad Autónoma de Buenos Aires y sus alrededores. En estos casos, existe una clara responsabilidad de diversa naturaleza cuando los datos personales son difundidos, publicados, transmitidos o utilizados sin consentimiento de los afectados, o bien sin aplicar técnicas de distorsión visual que impidan la identificación de las personas captadas por estos medios de vigilancia.

6. Lawner, Kevin, "Post-Sept. 11th International Surveillance Activity- A Failure of Intelligence: The Echelon Interception System & the Fundamental Right to Privacy in Europe", *Pace International Law Review*, Vol. 14, Issue 2, 2002, p. 435 y ss.; Wright, Steve, "The Echelon Trail: An Illegal Vision", *Surveillance and Society*, Vol. 2/3, p. 198 y ss.

7. Balkin, Jack M., "The Constitution in the National Surveillance State", *Minnesota Law Review*, Vol. 93, Nº 17-18, 2008, p. 2; Blitz, Marc Jonathan, "The Fourth Amendment Future of Public Surveillance: Remote Recording and other Searches in Public Space", *American University Law Review*, Vol. 63, N° 1, 2013, p. 21 y ss.; Dwork, Cynthia y Mulligan, Deirdre K., "It's not privacy, and it's not fair", *Stanford Law Review On line*, Vol. 66, 2013, p. 35 y ss.

En 2013, Edward Snowden hizo público distintos documentos que probaban sin margen de dudas que la Agencia Nacional de Seguridad (por sus siglas en inglés NSA, *National Security Agency*) había realizado interceptaciones masivas de comunicaciones telefónicas que eran almacenadas para su posterior tratamiento, por lo que se creó de esa manera una inmensa base de datos que permitía reconstruir cualquier tipo de comunicación pasada; este programa había sido autorizado por la sección 215 del *USA Patriot Act*. Tales revelaciones dejaron al descubierto la operación más importante de intervenciones telefónicas realizadas en tiempos modernos y, al mismo tiempo, se comprobó que las agencias gubernamentales de seguridad están abocadas por lo general al control extrajudicial de los ciudadanos con la excusa de la prevención de delitos organizados, de acuerdo con la estrategia contraterrorista adoptada en el país del Norte.[8]

Esta situación generó la interposición de una demanda por parte de distintas asociaciones civiles que abogan por la plena vigencia de los derechos constitucionales, entre ellas la Unión Americana de Libertades Civiles (ACLU, por sus siglas en inglés), contra el accionar institucional de las agencias de inteligencia e instituciones nacionales de ese país (Dirección Nacional de Inteligencia, Agencia de Seguridad Nacional, Secretaría de Defensa, Agencia Federal de Investigaciones y la Fiscalía General de los Estados Unidos de América) por la interceptación masiva de comunicaciones telefónicas y su registro (*metadata*).[9]

De acuerdo con el gobierno, los registros solo daban cuenta de ciertos datos relacionados con los números de los abonados involucrados, la fuente de la llamada y su destino, además del tiempo de duración de la conversación. En cambio, los demandantes argüían que esos

8. Manes, Jonathan, "On line Service Providers and Surveillance Law Transparency", *The Yale Law Journal Forum*, 2016, p. 343 y ss.; Crampton, Jeremy, "Collect it all: National Security, Big Data and Governance", *GeoJournal*, agosto, 2015 (referencia: DOI 10.1007/s10708-014-9598); Setty, Sudha, "Surveillance, Secrecy, and the Search for Meaningful Accountability", *Stanford Journal of International Law*, Vol. 16, 2015, p. 69 y ss.; Bauman, Zygmunt *et al.*, "After Snowden: Rethinking the Impact of Surveillance", *International Political Sociology*, Vol. 8, 2014, p. 121 y ss. La información obtenida por medio del espionaje electrónico (*big data*) por parte de la Agencia Nacional de Seguridad (NSA) fue utilizada con fines diversos, entre ellos, espionaje industrial, proyecciones sobre las preferencias de los consumidores, opiniones políticas y pronósticos de los cambios del electorado.

9. "ACLU v. Clapper", 785 F. 3d 787, 813 (2d Cir. 2015).

datos personales eran suficientes para determinar las preferencias políticas, religiosas, sexuales o sociales del abonado. Según el § 215 de la citada USA Patriot Act, el director de la Agencia Federal de Investigaciones (FBI, por sus siglas en inglés), o la persona designada por este, es quien tiene atribuciones para solicitar autorizaciones de registro de comunicaciones personales al Tribunal de Vigilancia de Inteligencia Extranjera (*Foreign Intelligence Surveillance Court* o FISC), cuando existan sospechas razonables de su participación en una actividad terrorista, aunque en realidad el citado § 215 habilita también la incautación de documentos vinculados con tal actividad y que sean idóneos para suministrar información de interés a los servicios de inteligencia.

En este aspecto, la Corte federal juzgó que el citado § 215 no facultaba el registro de tamaña información sobre contactos telefónicos de manera indiscriminada en vista de un eventual uso en materia de contraterrorismo.

Sin embargo, existen en la actualidad técnicas de investigación propias del Derecho Procesal Penal que son mucho más agresivas e invasivas que la mera captación por medio de un sistema de vigilancia urbano instalado hoy en día en cualquier ciudad moderna. Estas técnicas de investigación penal son utilizadas por los organismos de seguridad y prevención para invadir el ámbito de privacidad de las personas sospechadas de la comisión de un delito. Justamente en el campo de la lucha contra el terrorismo es donde se ha evidenciado con mayor virulencia el empleo de este tipo de investigación electrónica de los sospechosos de pertenecer o simpatizar con una organización terrorista.

En este trabajo habremos de detenernos en la aplicación de los avances tecnológicos a las técnicas de investigación y vigilancia en el proceso penal. Por ejemplo, la determinación de las computadoras utilizadas para el tráfico de pornografía infantil requiere establecer la dirección electrónica (IP) de los usuarios de ese servicio para conocer el domicilio real registrado por la empresa prestadora. Este informe permite conocer la geolocalización de la terminal utilizada para la comisión del delito y así identificar a su usuario.

También la interceptación de comunicaciones electrónicas se ha convertido en la actualidad en una herramienta eficaz para descubrir la comisión de delitos. El seguimiento electrónico de los movimientos de un sospechoso mediante el uso de artefactos, dispositivos o simple-

mente satélites hace posible conocer los movimientos habituales de una persona, establecer sus relaciones sociales y preferencias religiosas o políticas mediante la infiltración a distancia en su computadora personal.

Distintas formas de acoso se materializan diariamente a través de las redes telemáticas, en especial el uso fraudulento de perfiles de usuarios que permiten acceder de manera virtual a menores de edad en las redes sociales con el propósito de preparar el terreno para una futura agresión sexual; de hecho, en nuestro país se registraron casos de contactos telemáticos con menores de edad (*grooming*) con un desenlace fatal.

En consecuencia, las distintas formas de manifestaciones delictivas que han crecido al calor de esta nueva forma de comunicación global y el carácter trasnacional que tiene una buena parte de estos delitos han obligado a las autoridades públicas a la adopción de una serie de medidas preventivas y de investigación, como analizaremos a continuación, luego de definir el sentido y el alcance del concepto de Derecho Penal Informático.

Concepto de Derecho Penal Informático

La criminalidad informática es un fenómeno criminal propio de esta sociedad de la información. Los adelantos tecnológicos alcanzados en el campo de la comunicación mediante la expansión omnipresente de los sistemas telemáticos en nuestra vida cotidiana han generado un ámbito propicio para la comisión de delitos.[10] Por lo general, en el Derecho Penal Informático se distingue el uso de terminales para la comisión de delitos (por ejemplo, defraudaciones) del ataque dirigido contra el sistema telemático en sí (delitos informáticos en sentido propio).[11]

10. Schmölzer, Gabriele, "Straftaten im Internet: eine materiell-rechtliche Betrachtung", ZStW 123, 2012, p. 709 y ss.

11. Sieber, Ulrich, *Straftaten und Strafverfolgung im Internet*, Gutachten C zum 69. Deutschen Juristentag, Beck, Múnich, 2012, C 18 y ss.; Hilgendorf, Eric; Frank, Thomas y Valerius, Brian, *Computer-und Internetstrafrecht*, Berlín, Springer, 2005, marg. 123; Schuh, Daniel, *Computerstrafrecht im Rechtsvergleich - Deutschland, Österreich, Schweiz*, Berlín, Schriften zum Strafrecht, Heft 228, Duncker & Humblot, 2012, p. 28; Arzt, Gunther; Weber, Ulrich; Heinrich, Bernd; Hilgendorf, Eric, *Strafrecht. BT*, 2. Aufl., Gieseking, Bielefeld, 2009, § 8, marg. 46; Romeo Casabona, Carlos María, "De los delitos informáticos al cibercrimen. Una aproximación conceptual y político-criminal", *El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales*, *op. cit.*, p. 6 y ss.

Cuando un usuario utiliza la computadora como medio para cometer un fraude informático, esta es solo un instrumento para la comisión del delito y no se diferencia mucho de otros medios. En cambio, cuando ese mismo usuario atenta contra la funcionalidad del propio sistema informático, por ejemplo, introduciendo un virus para destruir, alterar o ralentizar los programas de ejecución del sistema, o bien cuando el objeto de acción es un correo o mensaje electrónico, entonces el sistema telemático aparece como finalidad u objeto de la acción del autor; por lo tanto, resulta más adecuado referirse acá a la comisión de un delito informático en sentido estricto.[12]

Por lo general, los autores especialistas en esta materia tratan de modo lato ambas constelaciones de casos dentro del concepto de criminalidad informática, ya que en última instancia lo que caracteriza en ambos sentidos la infracción cometida es la intermediación de un sistema informático (medio u objeto). Lo cierto es que la estructura y el funcionamiento de los sistemas informáticos se han transformado, en nuestro mundo moderno, en una herramienta insustituible y eficaz para llevar adelante no solo un proceso multiplicador de la comunicación virtual, sino que también toda la infraestructura económica, política y social de la nueva sociedad de la información está sostenida de manera indisoluble por la vitalidad de los sistemas informáticos. De acá surge la necesidad de delimitar correctamente ambas zonas de influencia normativa, ya que en la moderna sociedad de la información los peligros crecientes contra esta novel forma de funcionalidad de la sociedad del riesgo justifican para algunos acudir a la ingeniería de los delitos de peligro abstracto y la tutela de bienes jurídicos colectivos difusos.[13]

En adelante habremos de abocarnos a analizar someramente algunas cuestiones puntuales relacionadas con las investigaciones por parte de organismos públicos de delitos cometidos mediante el uso abusivo de las computadoras y las redes telemáticas, haciendo foco

12. Hilgendorf, Eric, "Aktuelle Fragen des materiellen Computer- und Internetstrafrechts im Spiegel neuerer Gesamtdarstellungen", ZStW 118, 2006, p. 202 y ss.; Leman-Langlois, Stéphane, "Questions au sujet de la cybercriminalité, le crime comme moyen de contrôle du cyberespace commercial", *Criminologie*, Vol. 39, 2006, p. 63 y ss.; Puricelli, José L., "Informática y delito", *Derecho penal y Derecho procesal penal*, Homenaje a Carlos Alberto Contreras Gómez, Buenos Aires, Abeledo Perrot, 1997, p. 186 y ss.

13. Díez Ripollés, José Luis, "De la sociedad del riesgo a la seguridad ciudadana: Un debate desenfocado", RECPC 07-01, 2005, p. 3 y ss.

especialmente en la regulación procesal penal de algunos países y la doctrina judicial en torno al sentido, alcance y legitimidad de las interferencias electrónicas en el ámbito de la privacidad de las personas acusadas o sospechadas de haber cometido un delito.

Monitoreo *online* (*Durchsuchung*, §§ 102 a 110 del Código Procesal Penal alemán)

En el plano del Derecho Comparado, la Ley Procesal Penal alemana ha regulado en su cuerpo normativo nuevas técnicas de investigación de delitos, en especial orientadas a la prevención de atentados cometidos por organizaciones terroristas o con el fin de desbaratar las actividades de la delincuencia organizada, o bien simplemente a la búsqueda de pruebas de hechos delictivos que tienen por objeto a las redes telemáticas. En este caso, los autores utilizan los medios informáticos para cometer estafas, accesos indebidos a correos electrónicos o bases de datos, distribuir pornografía prohibida, cometer apología del delito, etcétera, siendo necesario implementar, en este caso, técnicas de investigación acordes con los tiempos modernos que se viven.

En este sentido, un sector de la doctrina penal viene denunciando desde hace tiempo que la política criminal adoptó una perspectiva preventiva de la mano de un Derecho Penal en expansión orientado no solo a sancionar conductas previas a la lesión de un bien jurídico, sino también autorizando la invasión del ámbito de privacidad de las personas sospechadas de la comisión de delitos mediante el uso de técnicas de vigilancia o seguimiento electrónico.[14]

El § 102 del StPO autoriza la inspección del domicilio o de las pertenencias de una persona sospechada de ser autor o partícipe de un hecho criminal, de encubrimiento de datos u objetos relacionados con la investigación o de favorecimiento personal. Esta norma fue modificada en diciembre de 2015[15] en el marco de una reforma procesal orientada hacia la extensión de las facultades de intervención del tráfico de datos y de

14. Neubacher, F., "An den Grenzen des Strafrechts-Stalking, Graffiti, Weisungsverstöße", ZStW 118, 2006, p. 855 y ss.; Wohlwend, Sebastian, "Die Durchsuchung, gerade bei Dritten nach § 103 Abs. 1 S. 1 StPO", HRRS 11/2015, p. 454 y ss.

15. BGBl. I, p. 2218, del 10/12/15.

telecomunicaciones de la autoridad frente al peligro de una inminente comisión de graves hechos criminales (§ 100g), entre los que se cuentan el delito de traición; los atentados contra la paz; el régimen democrático o la seguridad exterior; la constitución de una asociación criminal u organización terrorista; delitos sexuales; la posesión, adquisición y distribución de pornografía infantil y juvenil; delitos de homicidio y asesinato; delitos contra la libertad personal, etcétera. De acuerdo con esta reforma, se han ampliado las facultades de investigación de delitos complejos o especialmente graves al autorizar las interceptaciones de cartas, comunicaciones telefónicas o electrónicas (correos), allanamiento de morada de los sospechosos o terceros vinculados con ellos, que podrían aportar algún tipo de prueba sobre la comisión de un hecho criminal o su preparación. Se establece así un ámbito favorable para el monitoreo electrónico y el almacenamiento de datos personales de una persona sospechada de ser autor, partícipe o encubridor de un delito.

La Ley Procesal Penal alemana exige como presupuesto mínimo necesario la presencia de un grado de sospecha suficiente para activar judicialmente lo que podríamos denominar una búsqueda de medios de prueba en el ámbito informático que permita identificar al autor o comprobar la materialidad del hecho pesquisado. Estas técnicas de investigación con artefactos de infiltración del ámbito privado de la persona sospechada de haber cometido un delito, o en vía de preparación de uno, se concentran por lo general en la invasión del domicilio privado, ya que las autoridades policiales pueden ser habilitadas judicialmente para recurrir a cierto tipo de recurso tecnológico que permita una injerencia discreta en el ámbito personal del sospechoso.[16]

Precisamente, hace poco tiempo, el Tribunal constitucional alemán se expidió sobre el sentido y alcance de las medidas de investigación llevadas a cabo por la autoridad policial en un proceso por presuntos sobornos de funcionarios públicos que habrían autorizado ilegalmente la exportación de armas de fuego a México. En este caso, el Tribunal constitucional afirmó que el allanamiento del domicilio de

16. Kochheim, Dieter, *Cybercrime und Strafrecht in der Informations- und Kommunikationstechnik*, Beck, Múnich, 2015, p. 543 y ss.; Hauck, Pierre, *Heimliche Strafverfolgung und Schutz der Privatheit*, Veröffentlichungen zum Verfahrensrecht, Bd. 102, Mohr Siebeck, Tübingen, 2014, p. 422; Roxin, Claus; Arzt, Gunther y Tiedemann, Klaus, *Introducción al Derecho Penal y al Derecho Penal Procesal*, Barcelona, Ariel Derecho, 1989, p. 153.

uno de los involucrados exigía un estado de sospecha suficiente basado en la presunta comisión de hechos concretos y no meramente conjeturales, por lo que se anuló de esa manera las decisiones de las dos instancias anteriores que habían homologado medidas de injerencia en la casa de uno de los acusados.[17] También se ha declarado inválido el secuestro de drogas en el interior del domicilio del sospechado, cuando la orden judicial tenía por objeto el secuestro de un arma.[18]

En el trascurso de 2016, el Tribunal constitucional alemán también ha sido llamado a intervenir sobre la constitucionalidad de algunas leyes que autorizan la aplicación de este tipo de medidas de monitoreo electrónico, en particular respecto de las investigaciones realizadas en el ámbito de la actuación de organizaciones terroristas, ocasión en la que este alto tribunal convalidó la constitucionalidad de la Ley Antiterrorista de 2008,[19] en especial sobre las medidas de vigilancia personal, domiciliaria, postal, electrónica, registro de datos personales de individuos sospechados de pertenecer o simpatizar con esta clase de organizaciones criminales, o de grupos de personas que puedan representar un peligro para la seguridad nacional (§§ 20b, 20c, 20g, 20h, 20j, 20k, 20l, 20m, 20u de la *Gesetzes zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt vom 25. Dezember 2008*), entre otras.[20]

Por el contrario, se ha juzgado de inconstitucional el registro de domicilio realizado a un simpatizante de fútbol con el propósito de obtener alguna prueba incriminatoria de un hecho cometido por terceros mediante una pericia informática de su computadora. En este caso, un grupo de fanáticos de un equipo de fútbol se había apoderado de una bandera del equipo contrario a modo de trofeo; en consecuencia, el fiscal solicitó un registro domiciliario del afectado con el objeto de descubrir la identidad de los autores de esa sustracción mediante la ubicación de un *banner* utilizado por el grupo acusado. El fiscal tenía sospechas de que la persona contra la que se dirigía tal medida podía estar relacionada de manera indirecta con ese hecho. De acuerdo con los presupuestos del § 103 StPO, se realizó una inspección domiciliaria

17. BVerfGE, del 13/03/14 - 2 BvR 974/12.

18. BVerfGE, 2 BvR 876/06, del 28/09/06 (LG München I/AG München), BVerfG HRRS 2006, Nº 808.

19. BGBl. I, p. 3083.

20. BVerfGE, del 20/04/16 - 1 BvR 966/09.

con la finalidad de obtener pruebas sobre la identidad de los autores del hecho investigado. En este caso, el tribunal constitucional alemán le dio la razón al quejoso, por entender que esa medida procesal había sido adoptada sobre la base de meras presunciones que no lograban satisfacer el test de razonabilidad para legitimar tal injerencia en el ámbito personal del damnificado, en especial cuando él no estaba sospechado de haber participado en la comisión del hecho.[21]

También este Tribunal constitucional ha anulado registros domiciliarios y de información personal almacenada en las computadoras, cuando esa medida judicial resulta desproporcionada con el objeto del proceso, al afectar de manera intensa el ámbito privado de las personas alcanzadas por tales medidas de injerencia estatal.[22]

Respecto de la infiltración de sistemas informáticos mediante el uso de dispositivos idóneos de rastreo y registro de comunicaciones electrónicas, el Tribunal constitucional alemán ha dicho que la investigación *online* solo puede justificarse en función de la importancia de los bienes jurídicos amenazados por un peligro inminente, en particular cuando esa conducta es idónea para lesionar la vida, la integridad y la libertad personales, o aquellos bienes jurídicos colectivos que pongan en peligro el fundamento o la existencia del Estado, o las condiciones de existencia de las personas. Este monitoreo *online* solo puede ser autorizado por el juez competente. En este caso se discutió la validez constitucional de una ley sancionada por uno de los *Länder* que componen la República alemana que había autorizado este tipo de medidas de vigilancia *online* respecto de las actividades desarrolladas por los integrantes de organizaciones terroristas. Previo a ello, en una anterior intervención de este tribunal superior se había declarado inconstitucional una ley dictada por este mismo *Land* con un alcance parecido.[23] A raíz de esta ley, se habían autorizado distintas medidas de vigilancia contra personas sospechosas de tener relaciones o simpatizar con grupos extremistas violentos, lo que generó la impugnación de distintos artículos

21. BVerfGE, del 11/01/16 - 2 BvR 1361/13.

22. BVerfGE, del 30/07/15 - 1 BvR 1951/13. En particular, debe tenerse presente el precedente dictado por este tribunal constitucional en el caso del allanamiento sin orden judicial basado en el peligro en la demora. (BVerfGE, del 20/02/01 - 2 BvR 1444/00).

23. BVerfGE, del 27/07/05 - 1 BvR 668/04 (BVerfGE 113, 348).

de esta ley, cuestión sobre la cual el Tribunal admitió de modo parcial la falta de compatibilidad de esas normas con el texto constitucional.[24]

No son pocos los casos en los que los tribunales alemanes han declarado la invalidez de un monitoreo *online* que fueron sustanciados en infracción a la garantía de inviolabilidad del domicilio, de las comunicaciones electrónicas y los efectos (*v. gr.*, computadoras, discos rígidos), ya que el proceder de los funcionarios públicos violentó el derecho de autodeterminación informática del afectado, en particular cuando esas medidas procesales no respetan el principio de proporcionalidad del acto en razón del grado de intensidad de la injerencia en el ámbito privado de los sospechados y la gravedad de los delitos investigados, de acuerdo con lo previsto por el citado § 102 StPO.[25]

Por su parte, la Ley Procesal Penal española regula, como dijimos, medios de investigación consistentes en la interceptación de comunicaciones telefónicas y telemáticas. También se prevé la captación y grabación de comunicaciones orales, mediante la utilización de aparatos electrónicos, que mantenga el sospechoso en la vía pública o en otro espacio público, en su domicilio o en cualquier otro lugar cerrado (art. 588 *quater* a). La implementación de esta forma de investigación se encuentra restringida a los delitos castigados con una pena con un límite máximo de por lo menos tres años de prisión, delitos cometidos en el seno de un grupo u organización criminal y delitos de terrorismo (art. 588 *quater* b). Esta medida de extrema injerencia en el ámbito privado de la persona sospechada solo puede ser adoptada por pedido expreso del juez, quien tendrá a cargo el control de su ejecución.

En materia de doctrina judicial norteamericana, la Corte Suprema de Justicia y los tribunales inferiores han ido desarrollando una interpretación dinámica de la Cuarta Enmienda de la Constitución de ese país respecto del derecho a la privacidad frente a los registros y secuestros irrazonables por parte de la autoridad pública, en consonancia con lo establecido por los arts. 18 y 19 de nuestra Constitución Nacional. En especial, habremos de referirnos someramente por razones de espacio

24. BVerfGE, del 27/02/08 - 1 BvR 370, 595/07 (BVerfGE 120, 274). En este sentido, SIEBER, U., *Straftaten und Strafverfolgung im Internet*, C 104 y C 105.

25. BGHSt 18/06, decisión del 31/01/07, BGH HRRS 2007, Nº 197. Al respecto, Buermeyer, Ulf, "Die Online-Durchsuchung. Technischer Hintergrund des verdeckten hoheitlichen Zugriffs auf Computersysteme", HRRS 4/2007, pp. 154 y ss.

solamente a algunos precedentes en la materia acerca de la variada jurisprudencia de ese máximo tribunal sobre el sentido y alcance de este derecho constitucional. En este aspecto, el punto álgido de la discusión pasa por determinar el criterio material del concepto de "registros y secuestros irrazonables" utilizado por la citada Cuarta Enmienda, ya que la necesidad de una autorización judicial dependerá, en todo caso, de la existencia de una causa probable que habilite dicho registro de la persona, el domicilio, los papeles y efectos personales.[26]

En un breve excurso, la Corte Suprema de Justicia norteamericana adoptó una posición liberal en el precedente "Boyd v. United States",[27] ocasión en que este tribunal se afanó por distinguir los objetos y efectos que quedaban fuera del concepto de papeles privados o personales. Posteriormente, este tribunal interpretó el vocablo "búsqueda" (*search*) utilizado en la redacción de la Cuarta Enmienda para legitimar investigaciones policiales en las cuales la expectativa razonable de intimidad o privacidad no aparecía violentada en todo caso o por lo menos no abiertamente. Al respecto, este máximo tribunal federal convalidó en varias oportunidades procedimientos realizados por la fuerza de seguridad en el marco de la investigación de la posible comisión de delitos que colisionaban con una posible expectativa de privacidad de los afectados. Nos referimos puntualmente a aquellos procedimientos en los que la au-

26. Slobogin, Christopher; Schumacher, Joseph E., "Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at 'Understandings Recognized and Permitted by Society'", *Duke Law Journal*, Vol. 42, Nº 4, 1993, p. 727 y ss.

27. 116 U.S. 619. En este sentido, "Mapp v. Ohio", 367 U.S. 643 (1961). Stewart, Potter, "The Road to Mapp v. Ohio and beyond: The Origins, Development and Future of the Exclusionary Rule in Search-and-Seizure Cases", *Columbia Law Review*, Vol. 83, Nº 6, octubre de 1983, p. 1365 y ss. En el precedente Mapp se estableció la regla de exclusión de la prueba obtenida de modo ilegal por los funcionarios públicos que habían allanado la morada de la demandante sin orden judicial. Nuestra Corte Suprema de Justicia de la Nación ha receptado esta doctrina en numerosos casos, cuando la autoridad pública allanó los domicilios de los imputados sin orden judicial, o bien al socaire del presunto consentimiento prestado por el afectado, quien ya se encontraba en calidad de detenido, entre ellos, Fallos: 308:733 ("Rayford"); 306:1752 ("Fiorentino"); 310:85 ("D'Acosta"); 311:2507 ("Romero"); 328:149 ("Ventura"). En un sentido opuesto, se cuentan los precedentes Fallos: 324:425 ("Fiscal vs. Fernández"), 324:3764 ("Adriazola").

toridad pública utilizó helicópteros,[28] aviones,[29] agentes encubiertos,[30] ingresó a lugares o espacios abiertos,[31] secuestró residuos[32] u objetos relacionados con la comisión de delitos hallados durante el registro de un automotor en el que viajaban los acusados como pasajeros,[33] o el pedido de informes bancarios[34] de la persona investigada para acreditar la causa probable exigida para la orden de allanamiento y arresto.

En todos estos casos, la Corte Suprema de Justicia norteamericana fue elaborando un criterio de "expectativa de privacidad razonable" desde distintos puntos objetivos y subjetivos; en especial ha tenido en cuenta dicha razonabilidad desde la perspectiva social o comunitaria. Esto último se aplicó en numerosos fallos para determinar si, desde la óptica de lo que la sociedad acepta como razonable, el registro y secuestro de efectos que acreditan la comisión de delitos sin orden judicial inobserva la expectativa de privacidad del afectado.

En el caso "California v. Greenwood", se afirmó que el registro y secuestro de material utilizado para el tráfico de estupefacientes obtenido del interior de las bolsas de residuos puestas en la vía pública por el interesado no ingresaba en el ámbito de la expectativa de privacidad razonable, ya que esa conducta importaba al menos el abandono de los elementos en la vía pública.

También en "California v. Ciraolo" el tribunal aplicó este criterio objetivo sobre lo que la sociedad acepta como razonable para legitimar

28. "Florida v. Riley", 488 U.S. 445, 1989.

29. "California v. Ciraolo", 476 U.S. 207, 1986.

30. "United States v. White", 401 U.S. 745, 1971. Sobre el cuestionado método de autoincriminación mediante engaño en el Derecho Procesal Penal alemán gracias a la intervención de terceros, cfr. Roxin, Claus, "Libertad de autoincriminación y protección de la persona del imputado en la jurisprudencia alemana reciente", *Estudios sobre justicia penal*, Homenaje al profesor Julio B. J. Maier, Buenos Aires, Editores del Puerto, 2005, p. 421 y ss.

31. "Oliver v. United States", 466 U.S. 170, 1984.

32. "Hester v. United States", 265 U.S. 57, 1924; "California v. Greenwood", 486 U.S. 35, 1988. En este sentido, se han pronunciado los tribunales inferiores, "United States v. Reicherter", 647 F. 2d 397 (3th Cir. 1981); "States v. Vahalik", 606 F. 2d 99, 101 (5th Cir. 1979); "United States v. Crowell", 586 F.2d 1020 (4th Cir. 1978); "United States v. Shelby", 573 F.2d 971 (7th Cir.); "Madga v. Benson", 536 F.2d 111 (6th Cir. 1976); "United States v. Mustone", 469 F.2d 970 (1st. Cir. 1972); "United States v. Dzialak", 441 F.2d 212 (2d. Cir), entre otros.

33. Rakas, 439 U.S. 128, 1978.

34. "United States v. Miller", 425 U.S. 435, 1976.

la inspección aérea llevada a cabo por funcionarios públicos con el propósito de detectar una plantación de marihuana. Dicho criterio material fue observado sobre el derecho a la privacidad de una persona detenida en el ámbito físico de su lugar de detención (celda).[35]

Almacenamiento temporario de comunicaciones

En consonancia con lo establecido por la Directiva 2006/24/EG, sobre Conservación de Datos de Tráfico en las Comunicaciones Electrónicas, del 15 de marzo de 2006, la Ley de Telecomunicaciones alemana establece en sus § 113a y § 113b la obligación para las empresas de telecomunicaciones de almacenar por el plazo de seis meses el tráfico de datos con la finalidad de poder ser utilizados en un proceso penal.[36] En España, se regula un deber homólogo de conservación de datos mediante lo dispuesto por la Ley Nº 25/2007, del 18 de octubre, cuyo artículo 3 define los sujetos alcanzados por tal deber de cooperación. En todos estos casos, esa información sobre el origen y destino de la comunicación, su contexto temporal y el tipo de servicio y comunicación utilizados debe ser suministrada por expresa orden de una autoridad competente.

En lo que respecta a la citada Directiva 2006/24/EC, ha sido declarada inválida por el Tribunal de Justicia de la Unión Europea en la decisión del 8 de abril de 2014.[37] La intervención de este tribunal comunitario obedeció a las consultas realizadas por el Tribunal Constitucional austríaco y la Corte Suprema irlandesa sobre la validez de esta directiva, en particular a la luz del derecho a la privacidad y el respeto de los datos personales garantizados por el artículo 8 de la Convención Europea de Derechos Humanos.

El Tribunal de Justicia europeo señaló que los deberes establecidos en la cuestionada directiva importaban una clara inobservancia

35. "Hudson v. Palmer", 468 U.S. 517, 1984.

36. Gerhold, Sönke, *Das System des Opferschutzes im Bereich des Cyber-und Internetstalking*, Nomos, Baden-Baden, 2010, p. 162; Arenas Ramiro, Mónica, "La protección de los datos personales en los países de la Comunidad Europea", *Revista Jurídica de Castilla y León*, N° 16, septiembre de 2008, p. 115 y ss.

37. D.O. 2014/ C 175/6, del 10/6/14. Sentencia del Tribunal de Justicia (Gran Sala) del 8 de abril de 2014, peticiones de decisión prejudicial planteadas por la High Court of Ireland, Verfassungsgerichtshof-Irlanda, Austria (Asuntos acumulados C-293/12 y C-594/12).

al derecho a la privacidad de las comunicaciones y al respeto de los datos personales, ya que se establecía como obligación la de informar la identidad de las personas que intervienen en la comunicación, el lugar y su duración y, por último, la frecuencia de las comunicaciones establecidas por dos personas en un plazo definido.

Desde el punto de vista del criterio teleológico seguido por la controvertida directiva comunitaria de adoptar herramientas técnicas para la lucha contra la criminalidad organizada o la comisión de delitos graves, el Tribunal de Justicia europeo estableció que su contenido resultaba desproporcionado a la luz de los fines perseguidos.

En particular, se discute si el pedido de información sobre la identidad del usuario de la dirección de IP involucrada o cualquier otro dato relacionado con el tráfico de datos por parte de los proveedores de servicios en la sociedad de la información debe ser oficiado por el juez competente o, en su caso, es suficiente con el pedido fiscal. En este aspecto, se encierra un dilema fundamental que consiste en definir el sentido y alcance de esa medida en el marco de un proceso penal.[38] No hay dudas de que el contenido de las comunicaciones almacenadas por los proveedores del servicio telemático en cumplimiento de la ley está alcanzado por el secreto de las comunicaciones y, así, solo por la vía de una orden judicial sería legalmente posible introducir esa información en el proceso penal sin menoscabar los derechos del acusado. Por lo general, los acusadores públicos solicitan informes a las empresas prestadoras de servicio en Internet sobre los datos personales de un usuario en particular, gracias a la detección de su dirección IP, lo que ha generado soluciones controvertidas sobre las facultades del fiscal para solicitar este tipo de informes, o bien si esa información integra el concepto de datos personales de un individuo, siendo necesaria en este caso la respectiva orden judicial.[39]

38. Gerhold, Sönke, *op. cit.*, p. 163. En el ámbito del Derecho alemán se discute si el pedido de informe sobre la dirección IP de un usuario determinado debe ser canalizado a través de los §§ 100g del StPO, en cuyo caso la orden judicial resulta ineludible, o de conformidad a lo previsto por el § 113 de la Ley de Telecomunicaciones de ese país, situación en la que no sería indispensable la citada orden judicial.

39. En el precedente "Acosta" (causa Nº 6790/15, resuelta el 20/04/16), la mayoría de los integrantes de la Sala II de la Cámara de Apelaciones en lo Penal, Contravencional y de Faltas del Poder Judicial de la Ciudad Autónoma de Buenos Aires (compuesta por los votos de los Dres. Delgado y Manes) declaró la nulidad de los informes solicitados

En particular, en el Reino Unido se dictó en 2000 la *United Kingdom's Regulation of Investigative Powers Act* (RIPA) que autoriza el almacenamiento de información doméstica y extranjera con el propósito de asegurar la seguridad interna y prevenir eventuales ataques terroristas. Esta ley crea tribunales especiales que garantizan el acceso a la justicia por parte de los particulares que puedan sentirse afectados por la aplicación de esta normativa. Esta ley fue armonizada posteriormente con el contenido y alcance de la citada Directiva 2006/24/EC, como respuesta a los ataques terroristas de Madrid y Londres. El gobierno británico ha introducido distintas reformas en la Ley de Inteligencia con el objeto de transparentar la actuación de los organismos de seguridad y visibilizar el funcionamiento de los tribunales especiales. Sin embargo, estos esfuerzos cayeron en saco roto cuando Snowden reveló las actividades ilegales cometidas por los servicios de inteligencia americano e inglés y la exposición del trabajo mancomunado de ambas agencias en materia de contraterrorismo, que incluyó el registro de millones de datos sensibles (correos electrónicos, imágenes captadas por las cámaras *web*, etc.). Posteriormente, el Comité de Seguridad, creado por el Parlamento para evaluar el trabajo de los Servicios de Inteligencia ingleses, concluyó que la información obtenida del uso de programas de espionaje y los registros de datos sensibles se ajustaba a los parámetros legales.[40]

Finalmente, como se dijo anteriormente, el Tribunal de Justicia europeo declaró que la citada Directiva 2006/24/EC era incompatible con la tutela al derecho a la privacidad de las personas.

En el caso americano, los organismos de seguridad apelaban a la Ley de Inteligencia de 1978 para registrar información sobre ciudadanos no americanos en el extranjero. De esta manera, se autorizaba a la interceptación de comunicaciones telefónicas de personas sospechadas de realizar actividades delictivas en perjuicio de intereses norteamericanos. Luego de los ataques terroristas de septiembre de 2001, se modificó la Ley de Vigilancia (Patriot Act) y en su lugar se exten-

por el fiscal respecto de la titularidad de las direcciones de IP de usuarios de Internet en un proceso sustanciado por la posible comisión del delito de distribución de pornografía infantil.

40. Setty, Sudha, *op. cit.*, p. 91 y ss.

dieron los poderes de los organismos de seguridad para interceptar comunicaciones de cualquier naturaleza y realizar el monitoreo de eventuales integrantes de organizaciones terroristas, lo que dio paso a una abusiva y masiva interceptación y almacenamiento de información originada en telecomunicaciones electrónicas, proporcionada por las empresas proveedoras de estos servicios. Posteriormente, como consecuencia de la revelación de secretos por parte de Snowden, la política contraterrorista fue forzada en cierta medida a modificar sus hábitos y dotar de mayor transparencia a la actuación de los organismos de seguridad. En particular, la enorme cantidad de información deducible de la base de almacenamiento y tratamiento de datos creados al calor de la lucha contraterrorista representa sin dudas el mayor esfuerzo del que se tiene conocimiento hasta ahora de registro de datos sensibles de miles y miles de personas sospechadas de tener algún tipo de vinculación con organizaciones terroristas.

La Ley Procesal Penal española también regula esta posibilidad de registro y almacenamiento masivo de información (arts. 588 *sexies*, incisos a, b y c). En este aspecto, el juez deberá autorizar el registro de los datos almacenados en las computadoras, instrumentos de comunicación y demás aparatos electrónicos del sospechoso. En la actualidad, un teléfono celular, un aparato electrónico cualquiera tiene la capacidad de almacenar información, imágenes, registros o datos que pueden ser de interés para la investigación judicial. Los datos almacenados en esos aparatos pueden ser útiles para determinar la posible intervención de terceros, así como los lugares físicos (geolocalización) o sitios en las redes telemáticas que fueron visitados por el sospechoso. Obviamente, el registro y tratamiento de esos datos deberá estar vinculado con el objeto del proceso penal. La autorización judicial de esta medida resulta inexcusable, pero en caso de urgencia se autoriza al examen directo de los datos contenidos en el dispositivo incautado (por ejemplo, en el caso del secuestro extorsivo para determinar la ubicación de la víctima, o en el de actividades de naturaleza terrorista para permitir la detección de bombas o prófugos, etc.).

Videovigilancia y supervisión electrónica (videocámaras y GPS)

Como dijimos al principio de este trabajo, existe un uso extendido de los sistemas de videovigilancia para controlar las actividades de los ciudadanos en la vía pública[41] y la de los trabajadores en sus puestos de trabajo, pero también la utilización de este sistema de seguridad se ha aplicado a las necesidades de seguridad y prevención de delitos. En la actualidad, se verifica la instalación cada vez más frecuente de medios de videofilmación concentrados en salas de monitoreo que permiten conocer en tiempo real el sentido y la intensidad del tráfico vial en los grandes centros urbanos, pero también supervisar el movimiento de miles de pasajeros que utilizan los medios de transporte público y privado. Esta vigilancia sempiterna al estilo orwelliano que hace algunas décadas parecía extraída de un cuento de ficción se ha hecho una realidad tangible.

En general, podemos subrayar que la instalación de sistemas de videocámaras en las empresas o comercios destinados a controlar el funcionamiento de la actividad laboral ha sido condicionada en muchos casos por la necesidad de su implementación, su idoneidad y la proporcionalidad de esa medida en función de los derechos personalísimos de los trabajadores.[42]

Existe consenso sobre la falta de expectativa razonable de privacidad en los lugares o espacios públicos, a partir de los lineamientos fijados en el precedente "Katz v. United States",[43] como veremos más adelante, cuestión que ha generado una extensa jurisprudencia sobre el sentido y alcance de esta doctrina, cuando el accionar de los funcionarios públicos se manifiesta en una supervisión o monitoreo de lugares públi-

41. Brown, Jeremy, "Pan, Tilt, Zoom: Regulating the Use of Video Surveillance of Public Places", *Berkeley Technology Law Journal*, Vol. 23, 2008, p. 759 y ss.

42. SSTCE 98/2000, del 10/04/2000; SSTCE 308/2000, del 18/12/2000; SSTCE 292/2000, del 30/11/2000; SSTCE 29/2013, del 11/02/2013.

43. Henderson, Stephen E., "Learning from All Fifty States. How to Apply the Fourth Amendment and Its State Analogs to Unreasonable Search", *Catholic University Law Review*, Vol. 55, 2006, p. 373 y ss., p. 377 y ss.

cos, por ejemplo, en la vía pública,[44] las veredas,[45] las tabernas,[46] jardines frontales,[47] pasillos de un establecimiento de depósito,[48] desfiladero,[49] campos abiertos,[50] y áreas comunes de baños públicos.[51]

En materia de investigación penal, el uso de artefactos o dispositivos electrónicos para el monitoreo de los movimientos de los sospechosos de la comisión de delitos, en especial, respecto del tráfico de estupefacientes, ha determinado decisiones jurisdiccionales cuestionables sobre el uso de estos instrumentos. El sistema de videovigilancia ha coadyuvado a identificar a los autores de los atentados terroristas en la ciudad de Oklahoma y Londres. En términos de costos, la instalación de sistemas de videomonitoreo resulta más económica que la vigilancia mediante recursos humanos desplegados en el lugar.[52]

La Ley Procesal Penal española regula de manera taxativa el uso de dispositivos técnicos de captación de imágenes, de seguimiento y de localización (art. 588 *quinquies*, incs. a, b y c). El registro remoto sobre equipos informáticos, es decir, el acceso remoto a la base de datos también se encuentra regulado por esta Ley Procesal Penal (arts. 588, incs. a, b y c). Estas medidas solo pueden ser adoptadas por el juez en casos concretos y de acuerdo con los principios rectores en la materia (art. 588 *bis*, inc. a). Una disposición interesante es la prevista por el artículo 588 (*septies*, inc. b), que establece el deber de colaboración de los titulares o responsables del sistema informático o base de datos objeto de registro, ya que ellos deberán prestar la colaboración necesaria para facilitar el acceso a la información almacenada en el dispositivo registrado.

Este deber de colaboración puede colisionar con derechos de propiedad intelectual de los titulares del sistema informático o del dispositivo electrónico en cuestión, como de hecho aconteció en el resonado caso de la empresa Apple ante el requerimiento del FBI de desbloquear

44. "McGray v. State", 581 A2d 45 (Md. Ct. Spec. App. 1990).
45. "State v. Augafa", 992 P. 2d 723 (Haw. Ct. App. 1999).
46. "Sponick v. Detroit Police Dept", 211 N.W. 2d 674 (Mich. Ct. App. 1973).
47. "State v. Holden", 964 P. 2d 318 (Utah Ct. App. 1998).
48. "State v. Bailey", (Del. Super. Ct. Nov. 30, 2001).
49. "United States v. Sherman", Nº 92-30067, 1993 U.S. App. (9th Cir. Mar. 13, 1993).
50. "State v. Costin", 720 A. 2d 866 (Vt. 1998).
51. "People v. Lynch", 445 N.W. 2d 803 (Mich. Ct. App. 1989).
52. Brown, Jeremy, *op. cit.*, p. 761.

el sistema de seguridad iOS instalado en el aparato celular perteneciente a uno de los agresores en el atentado terrorista cometido en San Bernardino (California), cuyo saldo fue la pérdida de vida de 14 personas. La Agencia de Investigación Federal le había solicitado a la firma Apple el desarrollo de un programa que le permitiera ingresar a la base de datos de los aparatos telefónicos distribuidos por esa empresa, pero sus responsables se negaron rotundamente por entender que ese programa podría ser utilizado por el gobierno de manera arbitraria y dejar expuesta la confidencialidad de los datos de sus usuarios. Luego de algunas semanas de litigio, el Buró Federal de Investigación logró acceder por sus propios medios a los datos almacenados en el celular del agresor.

También en el Derecho italiano es posible hallar legislación específica sobre la materia, en particular respecto del uso de imágenes, datos y archivos policiales obtenidos en el marco de videovigilancia urbana. La Ley N° 675/1996 procuró un punto de equilibrio entre la *riservatezza* (privacidad) y el uso de dispositivos de videovigilancia al crear una autoridad independiente integrada por cuatro legisladores de ambas cámaras, cuyas funciones son de distinta naturaleza y se canalizan en las atribuciones de inspección, recomendación, denuncia y comunicación a otros poderes en materia de protección de datos.[53]

A la par de los beneficios enumerados derivados del uso de videocámaras, se alzan voces en contra de su cada vez más extendida implementación, en especial, cuando asociaciones de defensa de los derechos individuales han objetado que la instalación de este tipo de videovigilancia atenta contra el derecho a la intimidad, en especial el derecho al anonimato y a la privacidad. La doctrina especializada se afana en señalar la vulneración de distintos derechos y garantías de los individuos, en particular la libertad de expresión, de reunión, de privacidad de las personas, de sus hogares, papeles y efectos contra registros y búsquedas irrazonables o arbitrarias, la garantía del debido proceso y el principio de igualdad de tutela.[54]

53. Martínez Martínez, Ricard, "Los ficheros de datos y archivos de imágenes policiales en la legislación italiana. Análisis de las resoluciones dictadas por el garante italiano para la protección de datos personales", *Revista Española de Derecho Constitucional*, Año 20, N° 60, sept.-dic. de 2000, p. 179 y ss.

54. Brown, Jeremy, *op. cit.*, p. 765.

A esto se suma la rampante evolución de los medios tecnológicos aplicados al uso de videocámaras cada vez más sofisticadas que permiten visualizar con mayor nitidez a las personas observadas desde un alcance extremadamente superior a la capacidad del ojo humano.

En un primer momento, el monitoreo de las actividades de un sospechoso de tráfico de drogas realizado mediante la interceptación de su *beeper* fue convalidado por la Corte Suprema de Justicia de los Estados Unidos de América, al afirmar que no existe una expectativa razonable de privacidad en la vía pública, en especial en el caso de quienes transitan por las autopistas.[55]

El uso de tecnología y la posible afectación del derecho a la privacidad también se consideraron en el caso "Kyllo v. United States",[56] ocasión en la que los integrantes del Máximo Tribunal federal debieron resolver si el uso de un aparato térmico para escanear una vivienda y determinar si el acusado poseía en su hogar una plantación de marihuana abastecida por lámparas de alto voltaje había infringido la expectativa de privacidad amparada por la Cuarta Enmienda de la Constitución federal.[57] Al respecto, la Corte hace una revisión del sentido y alcance del precedente Katz y sus derivaciones en función de los avances de la tecnología y la posibilidad cierta de acceder a áreas privadas (*v. gr.*, el domicilio), sin necesidad de realizar una injerencia corporal en ese ámbito. En este aspecto, el gobierno pretende distinguir una observación denominada *off the wall* (*sic* "fuera de la pared") para graficar aquella vigilancia realizada desde el exterior, de una vigilancia llamada *through the wall*, es decir, "a través de la pared", como aconteció en este caso, mediante el uso de aparatos tecnológicos. La Corte rechazó esa distinción,

55. "United States v. Knotts", 460 U.S. 276, 1983; "United States v. Karo", 468 U.S. 705, 1984.

56. 533 U.S. 27 (2001).

57. Clancy, Thomas K., "What Does The Fourth Amendment Protect: Property, Privacy, or Security", *Wake Forest Law Review*, Vol. 33, 2009, p. 307 y ss. Explica este autor que el fundamento originario de la Cuarta Enmienda de la Constitución norteamericana estuvo orientado hacia la tutela de la propiedad privada frente a los registros arbitrarios de la autoridad pública. La Cuarta Enmienda ha sido interpretada posteriormente en el precedente "Boyd v. United States" (116 U.S. at 635) a la luz de la prohibición de autoincriminación respecto del secuestro de papeles privados. En el caso "Olmstead v. United States" (277 U.S. 438), la Corte Suprema de Justicia de ese país restringió el alcance y sentido de la tutela constitucional a los objetos tangibles y contra la invasión física en el ámbito de privacidad individual.

ya que la tecnología actual aplicada a la inspección electrónica de las personas hace posible el uso de poderosos aparatos que permiten capturar las emisiones de voces realizadas en el interior del domicilio, así como el uso de satélites para observar dentro de las propiedades. De esta manera, concluye el Tribunal que el uso de aparatos de lectura térmica sin autorización judicial representó un atentado contra la intimidad del afectado y su expectativa razonable de privacidad.

A partir de la doctrina sentada en el precedente Katz, los tribunales americanos aplicaron el estándar de la expectativa razonable de privacidad en un sentido subjetivo y objetivo. El primero consiste en interrogarse si existía una expectativa razonable de privacidad desde el punto de vista del afectado. El segundo, en cambio, parte desde el aspecto objetivo de la cuestión al preguntarse si la sociedad reconoce como razonable esa expectativa.

Este baremo fue aplicado en el caso "California v. Ciraolo",[58] al resolver sobre la violación al derecho a la intimidad respecto de las imágenes fotográficas de la propiedad del acusado obtenidas desde una avioneta por parte de las autoridades policiales mediante el uso de una cámara fotográfica común. En este supuesto, se investigaba la posible existencia de una plantación de marihuana en el interior de un terreno que estaba cercado por un muro que imposibilitaba la vista desde el exterior. En consecuencia, el tribunal discutió el sentido y alcance del concepto *curtilage* (dependencias) respecto de la expectativa de privacidad del acusado frente a la arbitraria actuación de los funcionarios públicos.[59] Partiendo desde el desarrollo histórico de este concepto, la posición mayoritaria liderada por el juez Burger juzgó que las observaciones realizadas por los funcionarios públicos tuvieron lugar desde el espacio aéreo público, es decir, no existió acá una intromisión físi-

58. 476 U.S. 207, 1986.

59. Posteriormente, la Corte Suprema de Justicia de los Estados Unidos de América, en el caso "United States v. Dunn" (480 U.S. 294 [1987]), determinó que el vocablo "dependencias" de una vivienda requería la concurrencia de cuatro factores: la proximidad de dicho lugar con la vivienda, si esa área está incluida en el recinto circundante a la vivienda; la naturaleza del destino dispuesto para dicho lugar, y por último, la distancia que media de dicho recinto del área protegida de la vista de terceros. En esta hipótesis, se convalidó el ingreso de unos agentes de la DEA al campo de producción de los acusados y el intento de distribución de drogas y la observación del interior del granero donde se la fabricaba.

ca, ya que la plantación de marihuana era directamente visible desde la observación aérea llevada a cabo por los funcionarios públicos. En consecuencia, se validó esa observación y las imágenes fotográficas obtenidas de la plantación de marihuana, por lo que se aclaró que el precedente "Katz" invocado por la defensa no se aplicaba al caso acá juzgado, porque el desarrollo tecnológico futuro no tuvo incidencia en la resolución del caso, ya que la observación aérea se realizó a simple vista.

Anteriormente la misma Corte Suprema de Justicia había convalidado el uso de imágenes fotográficas obtenidas desde cámaras de fotos adaptadas con lentes de aumento.[60]

Posteriormente, esta doctrina judicial mutó en el precedente "United States v. Jones", en el que la mayoría de los integrantes del Máximo Tribunal federal de ese país consideraron que la supervisión prolongada de una persona sospechosa de participar en el tráfico de estupefacientes importaba una vulneración a la Cuarta Enmienda que tutela el derecho a la privacidad.[61]

Otro caso interesante de vigilancia se ventiló en el precedente "United States v. Cuevas-Pérez" resuelto por la Corte Suprema de Justicia de los Estados Unidos de América.[62] El señor Cuevas-Pérez estaba siendo investigado por tráfico de drogas por parte de las autoridades federales y con el propósito de registrar sus movimientos habituales instalaron un sistema de videocámaras en la proximidad de su domicilio y colocaron un GPS en su automóvil particular, todo ello sin orden judicial. Este dispositivo les permitía a los funcionarios conocer la ubicación del sospechoso y así determinar que había estado viajando con el vehículo monitoreado por distintos estados de la Unión. Al llegar a Illinois, el registro de batería baja del GPS obligó a los agentes federales a solicitar la cooperación de funcionarios locales para el seguimiento visual del sospechoso. Durante ese seguimiento, los funcionarios policiales detuvieron la marcha del acusado y le secuestraron más de un kilo de heroína del interior del automóvil gracias a la ayuda suministrada por canes entrenados. El acusado fue condenado a la pena de prisión de diez años por tráfico de estupefacientes. En esta sentencia,

60. "Dow Chemical Co. v. United States", 476 U.S. 227, 1985.

61. 132 S. Ct. 945, 2012. Al respecto, ver Setty, Sudha, *op. cit.*, p. 87.

62. 640 F. 3d 272 (7th Cir. 2011).

con expresa remisión al citado precedente "United States v. Jones", se concluyó que existió una violación al derecho a la privacidad amparado por la Cuarta Enmienda.

En cambio, se ha rechazado la violación al derecho a la privacidad, bajo los estándares fijados en "Katz", en la actuación de los funcionarios policiales que instalaron un dispositivo que registraba las llamadas recibidas por la víctima por parte de su acosador, ya que, a diferencia de lo acontecido en "Katz", dicho artefacto no tenía capacidad para registrar el contenido de las llamadas recibidas por la denunciante, sino que sólo se limitaba a registrar la cantidad de llamadas entrantes y la identificación del número de abonado.[63]

Como analizaremos más adelante, las últimas sentencias dictadas por la Corte Suprema americana en el caso de acceso no autorizado judicialmente a la información almacenada en dispositivos telefónicos de personas detenidas ("Riley v. California" y "United States v. Brima Wurie") generan cierto grado de optimismo en la lucha por la protección de los derechos personalísimos frente a la arbitraria injerencia estatal.[64]

Interceptación y monitoreo de comunicaciones telefónicas y telemáticas

Uno de los medios más frecuentemente utilizados en la investigación penal es la interceptación de medios y sistemas de comunicaciones.[65] En principio, la intervención de comunicaciones telefónicas representa una de las fuentes probatorias más corrientes en las leyes procesales penales. Las comunicaciones telefónicas y telemáticas están alcanzadas por el principio de confidencialidad, razón por la cual se hace necesario obtener una autorización judicial para proceder a la

63. "Smith v. Maryland", 442 U.S. 735, 1979.

64. Setty, Sudha, *op. cit.*, p. 87 y ss.

65. En nuestro país, la autoridad de aplicación en materia de interceptación y captación de comunicaciones ha ido mutando a lo largo del tiempo, pasando de la antigua Dirección General de Observaciones Judiciales dependiente de la Secretaría de Inteligencia de la Presidencia de la Nación (DOJ) a la Procuración General de la Nación del Ministerio Público (art. 17 de la Ley Nº 27126), para finalmente recalar bajo la órbita de la propia Corte Suprema de Justicia de la Nación, Departamento de Interceptación y Captación de las Comunicaciones (Dicom), con arreglo a lo dispuesto por el Decreto PEN Nº 256/2015.

intervención de los sistemas de comunicación para recabar información o vigilar las actividades de las personas sospechadas.

Ha sido objeto de un intenso debate la posibilidad de legitimar la intervención de las comunicaciones telemáticas sobre la base del dispositivo legal previsto para la interceptación de las comunicaciones telefónicas, porque las primeras involucran la codificación o encriptación de datos que hace necesaria la intervención de los sistemas informáticos de los participantes mediante el uso de *hackers*,[66] incluso la intervención de los proveedores del servicio en Internet para la interceptación de las comunicaciones electrónicas parece algo inevitable.[67] Sin embargo, la posterior reforma de la Ley de Telecomunicaciones alemana ha posibilitado la extensión de las tareas de monitoreo a los dispositivos electrónicos de comunicación.[68]

En consecuencia, como hemos mencionado en el caso de la Ley Procesal Penal alemana, a raíz de ciertos precedentes judiciales[69] que declararon la invalidez de este tipo de medidas de intromisión en las comunicaciones telemáticas de terceros sospechados de haber cometido un delito grave, generalmente agrupadas bajo la denominación

66. Sieber, Ulrich, *Straftaten und Strafverfolgung im Internet*, C 103 y C 104; Buermeyer, Ulf, "Die On line-Durchsuchung", "Technischer Hintergrund des verdeckten hoheitlichen Zugriffs auf Computersysteme", p. 158 y ss., en especial, p. 159 y ss.; Kemper, Martin, "Anforderung und Inhalt der On line-Durchsuchung bei der Verfolgung von Straftaten", ZRP 4/2007, p. 105 y ss.; Schantz, Peter, "Verfassungsrechtliche Probleme von 'On line-Durchsuchung'", KritV 3/2007, p. 311 y ss. Esta discusión sobre el sentido y alcance de la *On line-Durchsuchung* se ha trasladado al seno del Parlamento alemán, vid. BT-Drucks. 16/6535 (2007), p. 8; Rux, Johannes, "Ausforschung privater Rechner durch die Polizei- und Sicherheitsbehörden", JZ 6/2007, p. 285 y ss.

67. Klesczewski, Diethelm, "Straftataufklärung im Internet-Technische Möglichkeiten und rechtliche Grenzen von strafprozessualen Ermittlungseingriffen im Internet", ZStW 123, 2012, p. 737 y ss., p. 741 y ss.

68. *Klesczewski, Diethelm, op. cit.*, p. 743 y ss.

69. BGH 1 BGs 184/2006, decisión del 25/11/2006, HRRS 2007 Nº 466. En este caso, el tribunal superior alemán invalidó una intromisión en la computadora del prevenido con el propósito de copiar datos de su disco rígido, ya que no existían normas procesales que legitimaran esa facultad de la autoridad policial, intromisión que menoscabó la esfera de privacidad personal y el derecho a la autodeterminación informática del afectado. Esta decisión fue posteriormente homologada, BGH StB 18/06, decisión del 31/01/07. De otra opinión, BGH 3 BGs 31/06, 3 BJs 32/05 - 4 - (12) - 3 BGs 31/06, decisión del 21/02/06, HRRS 2007 Nº 468.

On line-Durchsuchung u *On line-Überwachung*,[70] lo que motivó una reforma procesal para admitirlas en su seno normativo, como ya hemos citado en la introducción de este trabajo.

Este monitoreo *online* incluye un conjunto de medidas de intromisión electrónicas que consisten en la copia remota de los datos almacenados en el disco rígido hasta el seguimiento telemático continuo del sospechado, que abarca el control sobre el tráfico de correo electrónico y sus contactos.[71] El uso de programas o sistemas informáticos intrusivos (*v. gr.*, *software* malicioso o troyanos) en el ordenador del monitoreado para registrar las pulsaciones en el teclado y así averiguar claves y contraseñas es una de las formas habituales de monitoreo electrónico (*Keylogging*). También el encendido remoto de micrófonos, cámaras o telefonía por Internet representan modos de monitoreo remoto de la conducta del afectado.[72]

En el caso de la interceptación y secuestro de correos electrónicos, el ordenamiento procesal penal de nuestro país ha sido diseñado sobre la base del documento físico, mas no del electrónico. En consecuencia, las normas procesales penales que reglamentan el artículo 18 de la Constitución Nacional deberían invariablemente adaptarse a esta nueva realidad, ya que en estos casos intervienen terceros, es decir, los proveedores del sistema, cuya participación puede ser insoslayable para materializar este tipo de medidas de injerencia. Al respecto, las normas procesales penales de países europeos han sido armonizadas para obligar a los proveedores de este servicio electrónico de alcance mundial a suministrar esos correos electrónicos y demás datos de interés para la investigación en curso.

El artículo 10, en el primer párrafo de la Ley Fundamental alemana, establece la garantía de inviolabilidad del secreto epistolar, así como del secreto postal y de las telecomunicaciones. En términos análogos se pronuncia nuestro artículo 18 de la Constitución Nacional. En

70. Mitsch, Wolfgang, *Medienstrafrecht*, Springer, Berlín, 2012, p. 214; Hauck, Pierre, *op. cit.*, p. 420 y ss.; Buermeyer, Ulf, *op. cit.*, "Technischer Hintergrund des verdeckten hoheitlichen Zugriffs auf Computersysteme", p. 154 y ss.

71. Mitsch, Wolfgang, *op. cit.*, p. 214; Schlegel, Stephan, "Beschlagnahme von E-Mail-Verkehr beim Provider", HRRS 2/2007, p. 44 y ss.; Klesczewski, Diethelm, *op. cit.*, p. 737 y ss. En este sentido, BGH 3 BGs 31/06, 3 BJs 32/05 - 4 - (12) - 3 BGs 31/06, decisión del 21/02/06, HRRS 2007 Nº 468.

72. Buermeyer, Ulf, *op. cit.*, p. 160 y ss.; Kemper, Martin, *op. cit.*, p. 106 y ss.; Schantz, Peter, *op. cit.*, p. 311 y ss.

función de ello, se ha discutido en el tribunal constitucional alemán si los correos electrónicos estaban alcanzados por esta garantía de inviolabilidad, cuestión que adelantamos fue saldada de modo favorable al reconocer mediante una interpretación dinámica que esos correos ingresaban en el ámbito de protección de aquella norma constitucional.[73]

Haciendo un estudio comparado sobre el sentido y alcance de las atribuciones de los poderes públicos para disponer de la interceptación de comunicaciones telefónicas de personas sospechadas de la comisión de delitos, la Corte Suprema de Justicia norteamericana interpretó de manera inicial en el precedente "Olmstead v. United States"[74] que la protección otorgada por la Cuarta Enmienda de la Constitución federal de ese país al ámbito de privacidad personal se limitaba a los objetos tangibles (personas, vivienda, papeles y efectos), pero no abarcaba las conversaciones, ya que en ese caso se discutía la validez de las escuchas telefónicas realizadas por la autoridad pública gracias a la interceptación de las líneas telefónicas ubicadas en el exterior del domicilio del acusado. Lo segundo en trascendencia de este fallo consistió en la afirmación de que la tutela de la privacidad personal solo comprendía la intrusión física en el domicilio del afectado, mas no la intervención de las citadas líneas telefónicas ubicadas, como se dijo, en el exterior de la vivienda.[75]

Al respecto, a la condición insoslayable de la autorización judicial se le suma la necesidad de que tal medida judicial sea proporcional a los fines de la pesquisa, de lo contrario, si ella no fuera necesaria o idónea respecto de la naturaleza del delito, podría ser tachada de inválida.

La identificación previa de los usuarios y titulares de los medios de comunicación interceptados no constituye una condición de validez de la medida judicial. En la doctrina judicial española, existe una consolidada postura que sostiene que esa condición de identificación previa de los usuarios o titulares del servicio de comunicación

73. BVerfGE 46, 120; BVerfGE 115, 166; BVerfGE 124, 43; Schlegel, Stephan, *op. cit.*, p. 44 y ss.; Schantz, Peter, *op. cit.*, p. 314 y ss.

74. 277 U.S. 438 (1928).

75. Clancy, Thomas K., *op. cit.*, p. 316 y ss. De esta manera, la Corte Suprema de Justicia de ese país adopta la teoría estricta o literal del concepto de propiedad abandonando así la línea interpretativa más amplia o liberal seguida en "Boyd v. United States". Posteriormente, esta exégesis literal o restrictiva fue dejada a un lado en el famoso precedente "Katz v. United States", de 1967.

cuya intervención judicial se ha solicitado no es un obstáculo legal válido para obtener esa medida.[76]

En cuanto a la necesidad de fundamentación de la resolución judicial que así lo ordena, ella debe ser autosuficiente, aunque también se acepta por lo común que su fundamentación puede reconstruirse a partir de las constancias agregadas al expediente.[77]

Las autoridades gubernamentales han aplicado, por lo general, la misma estrategia en la lucha contra el terrorismo al registrar una colosal masa de información suministrada por actores privados (compañías telefónicas, proveedores de servicios en Internet) en vista de futuras imputaciones penales. Esta forma de actuación agresiva por parte de los organismos de seguridad ha generado al mismo tiempo un sinnúmero de cuestionamientos por parte de los propios obligados a suministrar esa información, o bien gracias a la intervención de asociaciones civiles que intentan proteger el libre ejercicio de los derechos fundamentales sin la arbitraria y desproporcional injerencia estatal.[78]

Luego de los ataques terroristas de 2001, los gobiernos de los principales países atacados optaron por redoblar los esfuerzos en la lucha contra el terrorismo internacional, en especial, al sancionar una panoplia de leyes que autorizaban a las agencias de inteligencia y seguridad el registro de movimientos de potenciales autores de hechos criminales relacionados con actos terroristas. De esta manera, se cristalizó un incremento sensible de normas y leyes penales destinadas a estrechar los lazos contra el financiamiento del terrorismo, tipificar nuevos delitos y aumentar la presión contra el derecho a la confidencialidad de las comunicaciones.[79]

Al principio, los intentos de frenar esta embestida contra los derechos fundamentales de las personas fueron frustrados desde los tribu-

76. SSTS, 309/2010, del 31 de marzo; 493/2011, del 26 de mayo; 712/2012, del 26 de septiembre; 48/2013, del 23 de enero; 138/2015, del 13/3/15; SSTC 150/2006, del 22 de mayo y 104/2006, del 3 de abril.

77. SSTS 251/2014, del 13 de abril; SSTC 200/1997; 166/1999; 171/1999; 126/2000; 299/2000; 138/2001; 202/2001; 184/2003; 261/2005; 136/2006; 197/2009; 5/2010; 26/2010, entre otras. En la doctrina nacional dicha situación fue consolidada por la Corte Suprema de Justicia de la Nación en el precedente "Minaglia", del 4/9/07 (Fallos: 330:3801).

78. Manes, Jonathan, "On line Service Providers and Surveillance Law Transparency", p. 345; Setty, Sudha, *op. cit.*, p. 72 y ss.

79. Balkin, Jack, "The Constitution in the National Surveillance State", p. 1 y ss.

nales al refrendar las amplias atribuciones de los poderes públicos para actuar contra sospechosos de actividades terroristas ubicados en el extranjero, en especial, al acudir a las técnicas de vigilancia y seguimiento de personas extranjeras. En este sentido, la Corte Suprema de Justicia de Norteamérica convalidó en el caso "Clapper v. Amnesty International USA"[80] la aplicación del § 1881a del Foreign Intelligence Surveillance Act de 1978 (FISA), que faculta al Procurador General y al Director Nacional de Inteligencia para el seguimiento y vigilancia de ciudadanos no americanos residentes en el extranjero con el objeto de buscar y almacenar información sobre actividades ilícitas; en particular la demanda se centraba en la confidencialidad de las comunicaciones interceptadas por ese organismo de inteligencia. En este caso, la Corte Suprema de Justicia de ese país rechazó la demanda de las asociaciones civiles sobre la base de la falta de acreditación de un caso judicial, ya que el perjuicio que podría ocasionar la aplicación del citado § 1881a de la FISA no era uno de naturaleza concreta ni estaba individualizado o bien no era actual ni inminente.

A estas alturas debemos recordar que en 1978 el Congreso federal de ese país sancionó la Ley de Vigilancia de Inteligencia Extranjera con el propósito de buscar información sobre actividades ilegales llevadas a cabo por personas de nacionalidad extranjera contra los intereses de los Estados Unidos de América. Esta ley autorizaba el monitoreo electrónico de presuntos sospechosos ubicados en jurisdicciones foráneas. Se crearon dos tribunales especiales para autorizar este tipo de vigilancia, uno de ellos fue la Corte de Vigilancia de Inteligencia Extranjera. Al mismo tiempo se puso en funcionamiento un tribunal superior para revisar los pedidos denegados de autorizaciones de monitoreo electrónico por parte de los organismos de inteligencia involucrados.

Sin embargo, la competencia de estos tribunales especiales siempre ha estado en el ojo de la tormenta, ya que su actividad no solo está rodeada de un alto secretismo, sino que, además, se ha cuestionado la forma de designación de sus integrantes, su capacidad para controlar y limitar la actuación de la Agencia Nacional de Seguridad, puesto que la información recibida para decidir la procedencia o no de una vigilancia o monitoreo no solo proviene de la misma fuente interesada,

80. "Clapper v. Amnesty International USA", 133 S. Ct. 1138, 2013. En este sentido, "Al-Haramain Islamic Found v. Bush", 507 F. 3d 1190 (9th Cir.2007); "Al-Haramain Islamic Found v. Obama" 705 F. 3d 845 (9th Cir. 2012). Al respecto, Setty, Sudha, *op. cit.*, p. 85 y ss.

sino que ella es, por lo general, demasiado escueta o vaga como para poder formarse de una idea aproximada de la relevancia del caso.[81]

Después de los ataques del 11 de septiembre de 2001, la administración de Bush orientó e intensificó esa actividad de control y monitoreo electrónicos contra la organización Al-Qaeda, sus integrantes y cualquier otro grupo asociado a ella. Este programa de contraterrorismo fue conocido como *Terrorist Surveillance Program* (TSP) y daba carta de ciudadanía a la interceptación de cualquier tipo de comunicación realizada en el extranjero por parte de quienes hubiesen sido sospechosos de pertenecer a la citada organización terrorista internacional. Este programa fue objetado por asociaciones civiles por temor a la interceptación de comunicaciones realizadas por ciudadanos americanos hacia el extranjero, en especial, por las actividades realizadas por periodistas, abogados y académicos, ya que el derecho a la confidencialidad de sus comunicaciones quedaba directamente menoscabado por el funcionamiento del citado programa de escuchas. Por su parte, la Agencia de Inteligencia argumentó que la demanda debía ser rechazada, ya que la información solicitada estaba amparada bajo la Ley de Seguridad Nacional, cuya divulgación estaba prohibida por ley. En general, las Cortes federales rechazaron las acciones judiciales tendientes a encorsetar el ejercicio abusivo de las atribuciones de investigación por parte de las agencias de inteligencia basadas en el argumento de la falta de agravio o de caso judicial.[82]

Esta tendencia, sin embargo, parece haber dado un giro importante en el precedente "Klayman v. Obama",[83] en el que el tribunal federal de segunda instancia reconoció por primera vez que los procedimientos llevados adelante por la Agencia Nacional de Seguridad habían infringido la Cuarta Enmienda (derecho a la privacidad).[84]

Uno de los casos más renombrados ha sido la lucha legal que insumió más de once años por parte del titular de una pequeña empresa

81. Setty, Sudha, *op. cit.*, p. 82 y ss.

82. "ACLU v. NSA *et al.*", 493 F. 3d 644 (6th Cir. 2007). Esta decisión fue homologada el 19 de febrero de 2008 por la Corte Suprema de Justicia de ese país al rechazar la apelación de los demandantes.

83. 957 F. Supp. 2d 1, 9 (D.D.C. 2013).

84. Nakashima, Ellen, "After 11 Years, a Curtain Is Lifted on a Secret FBI Demand for a Target's Data", *Washington Post* (30/11/2015). Disponible en: https://www.washingtonpost.com

proveedora de servicios en Internet que había sido intimado por el FBI a aportar datos sensibles sobre usuarios del servicio. El requerido intentó publicar el contenido de la intimación recibida bajo el amparo del ejercicio del derecho a la libertad de expresión, pero el organismo federal buscó por medios legales impedir tal difusión. Este proceso sirvió para exponer el sentido y alcance de las normas sobre seguridad nacional, en especial cuando la naturaleza de la información requerida de los clientes del servicio puede servir para descubrir sus preferencias políticas, religiosas, sexuales, sociales y familiares, es decir, contienen una cantidad de datos sobre la vida personal de los usuarios que atenta de manera directa contra la confidencialidad de esa información.

En la actualidad, el mencionado § 215 ha sido finalmente modificado gracias a la primera ley sobre vigilancia que pretende limitar los poderes públicos sobre el registro de llamadas telefónicas y electrónicas. La *USA Freedom Act*[85] fue sancionada el pasado año (2015) con el propósito de regular el registro y el monitoreo electrónicos para obtener información útil en la lucha contra el terrorismo y demás actividades criminales. En general, se establece un límite de 180 días de vigilancia, luego del cual será necesario contar con autorización judicial.

En síntesis, podemos afirmar que los gobiernos han ampliado el horizonte de aplicación de los métodos de monitoreo electrónico de potenciales autores de delitos, en principio relacionados con asociaciones terroristas, para posteriormente intensificar y extender su uso hacia otros sectores de la criminalidad organizada. Las distintas administraciones han argumentado la necesidad, la importancia y la eficacia de este tipo de programas de vigilancia electrónica de las comunicaciones de terceros, aunque otro sector de la política y de las asociaciones civiles han alertado sobre los peligros reales que corren los derechos fundamentales, cuando el Estado y sus distintas agencias de seguridad aplican de manera sistemática esta forma de espionaje y así habilitan las injerencias arbitrarias en el ámbito privado de los ciudadanos con el lema de la doctrina de la seguridad nacional.[86]

85. United and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring (USA Freedom), Act of 2015, publ. L. N° 114-23, 129 Stat. 268 (50 U.S.C. §§ 1872-1874, 2012, y 18 U.S.C. §§ 2280-2281, 2332, 2012.

86. Setty, Sudha, *op. cit.*, p. 76 y ss.

La inviolabilidad de datos sensibles almacenados en dispositivos electrónicos por parte de la autoridad pública (el caso de la telefonía celular)

La garantía de inviolabilidad de la correspondencia epistolar y los papeles privados consagrada en nuestro artículo 18 de la Constitución Nacional y en numerosos convenios y tratados internacionales (art. 11, párrafo 2, de la CADH, art. 17 PIDCyP, art. 12 DUDH, art. X de la Declaración Americana de los Derechos y Deberes del Hombre) ha sido objeto de una interpretación dinámica que permite su aplicación actual en consonancia con los tiempos modernos. Si bien los constituyentes solo pudieron tener en cuenta respecto del contenido de esta garantía las cartas y demás papeles privados de una persona, lo cierto es que la Corte Suprema de Justicia americana ha extendido esta garantía a los datos almacenados en el teléfono celular de una persona detenida. El 25 de junio de 2014 ese Tribunal resolvió, en los casos "Riley v. California"[87] y "United States v. Brima Wurie",[88] sobre el alcance de las facultades de los funcionarios policiales para examinar sin autorización judicial el contenido de la información del teléfono celular de una persona detenida. De esta forma, en estos novedosos e importantes *leading cases*, la Corte Suprema de Justicia americana ha juzgado que ese procedimiento policial violó la Cuarta Enmienda de la Constitución americana, *inter nos*, el artículo 18 de la Constitución Nacional y la "garantía de inviolabilidad de la correspondencia epistolar y los papeles privados".

Si bien es cierto que la Corte Interamericana de Derechos Humanos ya se expidió sobre la garantía de inviolabilidad, en especial vinculada con la difusión pública de conversaciones privadas[89] y nuestro máximo tribunal hizo lo propio en el caso pionero "Charles Hnos".[90] A partir de ahí, se desarrolló una línea jurisprudencial que resaltó la importancia del contenido de la esfera de privacidad, su

87. 573 U.S. 132, 2014.

88. 573 U.S. 212, 2014.

89. "Caso Escher y Otros vs. Brasil", sentencia del 6/07/09.

90. Fallos: 46:36, del 5/09/91.

materialización en las comunicaciones privadas y la necesidad de delimitar la injerencia pública.[91]

En especial, se ha afirmado:

> El derecho a la privacidad comprende no solo la esfera doméstica y el círculo familiar y de amistad, sino otros aspectos de la personalidad espiritual o física de las personas, tales como la integridad corporal o la imagen, nadie puede inmiscuirse en la vida privada de una persona ni violar áreas de su actividad no destinadas a ser difundidas, sin su consentimiento o el de los familiares autorizados para ello, y solo por ley podrá justificarse la intromisión, siempre que medie un interés superior en resguardo de la libertad de los otros, la defensa de la sociedad, las buenas costumbres o la persecución de un crimen.[92]

Por lo demás, la esfera de privacidad se extiende también al contenido de las comunicaciones telefónicas, telemáticas y los datos almacenados en las computadoras personales. Las comunicaciones telefónicas siempre han sido naturalmente objeto de interceptaciones y registros ilegales, por lo que la tutela jurídica también alcanzó a las comunicaciones de naturaleza laboral.[93] O bien cuando el gobierno intercepta el correo o las comunicaciones de una persona de modo meramente preventivo,[94] o cuando dicha intervención resulta irrazonable,[95] incluso cuando las llamadas privadas se realizaron mediante un sistema interno de comunicación operado por la autoridad policial.[96] El acceso a los informes del servicio social de una persona[97] o la interceptación de los mensajes personales[98] también ingresan en el ámbito de tutela del derecho a la privacidad.

---

91. Fallos: 318:1894. D. 346. XXIV. "Dessy, G. G. s/ hábeas corpus", del 19/10/1995 y Fallos: 332:111. "Halabi, Ernesto c/ PEN –Ley Nº 25873, dto. 1563/04 s/ amparo Ley Nº 16986", H. 270.XLII, del 24/02/2009 y, últimamente, Fallos: 333:1764 (Quaranta, J. C. s/ inf. Ley 23.737), del 31/08/2010.

92. CSJN, Fallos: 316:703, "Gutheim v. Alemann", del 15/03/1993.

93. TEDH, "Amann v. Switzerland [GC]", Nº 27798/95, 16/02/2000, para. 65.

94. Ibídem, "Malone v. The United Kingdom", del 2/08/1984, Series A, Nº 82.

95. Ibídem, "Lambert v. France", del 24/08/1998, Reports of Judgments and Decisions 1998-V.

96. Ibídem, "Halford v. The United Kingdom", del 25/07/1997, Reports of Judgments and Decisions 1997-III.

97. Ibídem, "M. G. v. The United Kingdom", del 24/09/2002, Nº 39393/1998.

98. Ibídem, "Taylor-Sabori v. The United Kingdom", del 22/10/2002.

La interceptación de los medios de comunicación en general ha sido considerada legítima cuando existe un interés superior que tutelar. Por ejemplo, la Ley de Seguridad alemana autorizaba el registro de ciertas comunicaciones;[99] no obstante, esa pesquisa tiene un límite razonable cuando los servicios de inteligencia actúan de modo preventivo al almacenar datos personales sin posibilidad de refutar su contenido por parte del afectado.[100]

En síntesis, podemos concluir que el derecho a la intimidad de una persona abarca todos los aspectos esenciales (personales, familiares, laborales, sociales, religiosos, médicos, etc.) de la manifestación de su personalidad. La intromisión estatal en la esfera de privacidad de una persona debe estar debidamente autorizada y sometida al control judicial, el que deberá realizar un examen pormenorizado de las razones de necesidad, razonabilidad y proporcionalidad invocadas por la autoridad pública para acceder a los datos personales de un individuo. A continuación pasaremos a analizar brevemente los pasajes más importantes de la decisión judicial mencionada en el título de este trabajo que se relaciona con los datos almacenados en un celular de una persona previamente detenida y si existen motivos de urgencia para justificar su requisa y examen sin control judicial.

En lo que aquí interesa, los integrantes de la Corte Suprema norteamericana consideraron que el examen del contenido de los datos almacenados en el celular de una persona que se encontraba detenida –en un caso por portación ilegal de armas de fuego ("Riley") y en el otro por su presunta conexión con el tráfico ilegal de estupefacientes ("Wurie")– debía ser precedido de una orden judicial que autorizara el registro de la información almacenada en los dispositivos secuestrados para su posterior utilización en el proceso en contra de los intereses de los acusados.

La información obtenida de esta pesquisa ilegal por parte de las autoridades locales permitió vincular a Riley con distintos actos cometidos por una pandilla callejera (The Bloods). Los funcionarios públicos revisaron el contenido de la información del *smartphone* de Riley y así obtuvieron acceso a la base de datos que lo conectaba con su pertenencia a esa banda callejera mediante las captaciones de fotos y videos

99. Ibídem, "Klass v. Germany", 6/09/1978, Serie A, Nº 28.

100. Ibídem, "Rotaru v. Romania", del 4/05/2000, aplicación Nº 28341/95.

almacenados en ese aparato celular. De esta manera, se le pudo atribuir a Riley su participación en un tiroteo y asalto, que había concluido con la muerte de una persona.

En el caso de "Brima Wurie", el hecho por el que esta persona fue detenida se justificó por su participación en el tráfico ilegal de drogas. En la estación de policía, los funcionarios le secuestraron dos teléfonos celulares. Luego, la policía detectó una serie de llamadas recibidas en uno de los celulares secuestrados, identificado su contacto como *"My house"*. El examen posterior de los celulares arrojó como resultado la dirección y el número de departamento de donde provenían las llamadas, lo que derivó en la detención de otra persona de sexo femenino (su esposa) y el secuestro de 215 g de distintos estupefacientes; para ello se obtuvo la correspondiente orden judicial de allanamiento y secuestro.

En el voto preopinante del *Chief Justice* Roberts (presidente de la Corte Suprema de los EE. UU.), se analiza el desarrollo histórico de la doctrina judicial de esa Corte en relación con el contenido y alcance de la garantía de la inviolabilidad de la correspondencia y los papeles privados frente a pesquisas y medidas irrazonables por parte de las autoridades públicas. Con cita del precedente "Chimel v. California",[101] donde se juzgó mediante el test de razonabilidad el allanamiento y requisa realizados en la casa del sospechoso sin contar con la debida autorización judicial, se dijo en esa oportunidad que los funcionarios públicos habían actuado de modo razonable, pues no habían violentado la Cuarta Enmienda, cuando esa pesquisa estuvo orientada a la búsqueda de armas de fuego para evitar que sean utilizadas contra los propios funcionarios o coadyuvar en la huida del acusado. También estaría justificado ese proceder de modo preventivo cuando el acusado podría destruir la evidencia del caso.

Esta doctrina judicial adoptada en el citado caso "Chimel" fue posteriormente seguida en el caso "United States v. Robinson",[102] cuando un funcionario policial interceptó la marcha del vehículo conducido por el causante y lo detuvo por manejar con la licencia vencida. Durante el procedimiento de detención, el funcionario requisó sus

101. 395 U.S. 752, 1969.

102. 414 U.S. 218, 1973.

pertenencias y secuestró de un atado de cigarrillos 14 cápsulas de heroína. Esta doctrina fue aplicada también en los casos "United States v. Chadwick"[103] y "California v. Acevedo".[104] Sin embargo, esta regla de interpretación fue dejada a un lado en el precedente "Arizona v. Gant",[105] por entender que la requisa de drogas sin orden judicial efectuada en el interior del automotor de una persona que ya se encontraba detenida no podía justificarse a la luz de los parámetros de razonabilidad utilizados en la mencionada doctrina "Chimel", y menos aún asirse de la doctrina "New York v. Belton"[106] aplicable para la requisa de automotores. El argumento fue precisamente que la condición de detenido del requerido no relevaba a las autoridades de su deber de contar con una orden judicial, puesto que en esa situación no existía peligro para los participantes de la detención ante una eventual reacción violenta del acusado y, menos aún, la posibilidad de destruir evidencia.

En los mencionados casos, los integrantes de la Corte Suprema se enfrentaron al desafío de valorar si el teléfono celular estaba alcanzado por la garantía de la Cuarta Enmienda, ya que ese aparato forma parte de la vida cotidiana, al extremo de que, como se dice en uno de los pasajes de la sentencia anotada, "un visitante de Marte podría concluir que es una parte importante de nuestra anatomía humana". La tecnología moderna ha impuesto el uso de celulares para prácticamente la totalidad de la población adulta. En cuanto a los estándares aplicados en el precedente "Chimel" respecto de la posibilidad de agredir a los funcionarios o la destrucción de evidencia, esos parámetros no pueden ser aplicados a la información almacenada (*digital data*) en los teléfonos celulares. En los casos "Ripley" y "Brima Wurie", el peligro de destrucción de evidencia era inexistente; en especial, se rechazaron los argumentos brindados sobre el peligro que podría representar que los acusados hayan encriptado la información. Sobre la posibilidad del uso del celular como arma, la Corte lo rechazó por infundado, ya que no existía peligro personal para los involucrados.

103. 433 U.S. 1, 15, 1977.
104. 500 U.S. 565, 1991.
105. 556 U.S. 7, 542, 2009.
106. 453 U.S. 454 (1981).

Los argumentos del Estado se concentraron en equiparar los datos almacenados en un celular a los demás objetos físicos, por ejemplo, se cita en apoyo de esta tesitura la requisa de paquetes de cigarrillos, la billetera o el monedero. Esta equiparación de tratamiento fue rotundamente descartada por el tribunal al señalar que los teléfonos celulares integraban una categoría de privacidad que va más allá de la prevista para los objetos mencionados, al distinguir que la inspección del contenido de los bolsillos de una persona aprehendida está vinculada racionalmente con el propio arresto, pero que la pesquisa no puede abarcar el contenido de los datos almacenados en el celular, ya que eso sería irrazonable para los estándares aplicados por la Corte. Se dijo:

> Los teléfonos celulares difieren en ambos sentidos, cualitativa y cuantitativamente, de otros objetos que podrían ser tenidos en cuenta en el arresto de una persona. El término "teléfono celular" es una engañosa forma abreviada en sí misma, puesto que muchos de estos aparatos son de hecho minicomputadoras, que también tienen la capacidad de ser utilizados como teléfonos. Ellos podrían ser fácilmente denominados como cámaras, videocámara, archivos de fichas giratorias, calendarios, grabadoras, bibliotecas, diarios, álbumes, televisores, mapas o cartas.

Y prosigue diciendo:

> Una de las más notables características de los modernos teléfonos celulares es su inmensa capacidad de almacenaje. Antes de la existencia de los teléfonos celulares, el registro de una persona estaba limitado generalmente por la existencia física y tendía a constituir una estrecha intrusión en la privacidad [...] La mayoría de las personas no pueden cargar consigo cada carta recibida en los últimos meses, toda foto que toman, o todo libro o artículo que leyeron, tampoco habría una razón para hacerlo. Y si lo hicieran, deberían arrastrar detrás de ellos un baúl que estaría sujeto a una orden judicial de requisa, como en el caso Chadwick, *supra*, en lugar de un recipiente del tamaño de un paquete de cigarrillos, como ocurrió en Robinson. Pero la posible intromisión en la privacidad no tiene la misma restricción física cuando se trata de teléfonos celulares. El celular más vendido actualmente tiene una capacidad estándar de almacenaje de 16 Gigabytes (y están disponibles con un almacenaje de hasta 64 GB). 16 Gigabytes se traducen en millones de páginas de texto, miles de fotos o cientos de videos [...] Los teléfonos celulares combinan esa capacidad con la habilidad

de almacenar muchas clases de información. Aun los teléfonos celulares más básicos que se venden por menos de veinte dólares pueden almacenar fotos, imágenes de texto, mensajes de texto, historial de Internet, un calendario, una agenda telefónica con miles de datos, etc. Nosotros esperamos que esta brecha entre la viabilidad física y la capacidad digital continúe ensanchándose en el futuro.

La capacidad de almacenaje de los teléfonos celulares tiene importantes consecuencias interrelacionadas para la privacidad. Primero, el teléfono celular registra en un solo lugar muchas formas distintas de información –una dirección, una nota, una receta médica, un balance bancario, un video– que revelan en combinación mucho más que un registro aislado. Segundo, la capacidad de los teléfonos celulares permite que un solo tipo de información revele mucho más de lo que antes era posible. La suma de la vida privada de un individuo puede ser reconstruida a partir de miles de fotografías etiquetadas con fechas, ubicaciones y descripciones; no puede decirse lo mismo de una o dos fotografías de seres queridos que se llevan en una billetera. Tercero, los datos almacenados en un teléfono celular pueden retrotraerse a la fecha de compra del teléfono o aun antes. Una persona puede llevar en su bolsillo un papel escrito para recordarle llamar a Mr. Jones. Ella no llevaría un registro de todas sus comunicaciones con Mr. Jones realizadas en el pasado como las que se guardan en un teléfono celular.

Finalmente, hay un elemento dominante que caracteriza a los teléfonos celulares, pero no a los registros físicos. Antes de la era digital, las personas no llevaban consigo información personal sensible. Ahora la persona que no lleva consigo un celular, "con todo lo que el celular contiene", constituye una excepción. De acuerdo con una encuesta, casi tres cuartos de los usuarios de teléfonos *inteligentes* informan que no se alejan más de dos metros de su teléfono celular, y el 12% admite que usa el teléfono en la ducha [...] Hace diez años los funcionarios policiales en el curso de una requisa podían ocasionalmente toparse con algún elemento muy personal como un diario íntimo [...] Pero esos hallazgos eran pocos y aislados. Por el contrario, en la actualidad no es una exageración decir que muchos de la mayoría del 90% de los adultos titulares de un teléfono celular portan consigo un registro digital de casi todos los aspectos de su vida personal –desde lo más mundano hasta lo más íntimo–. Permitir a los funcionarios policiales escrutar estos registros de modo rutinario es muy distinto a permitirles revisar uno o dos objetos personales.

Si bien los datos almacenados en un teléfono celular, se distinguen de los registros físicos por su cantidad, algunos tipos de datos son también

cualitativamente diferentes. Por ejemplo, un historial de búsquedas de Internet puede ser hallado en un teléfono con capacidad de navegación y puede revelar los intereses privados o preocupaciones de un individuo –así una búsqueda de los síntomas de una determinada enfermedad junto con las visitas frecuentes a la WebMD–. Los datos en un celular pueden revelar dónde estuvo una persona. El historial de información sobre la locación de una persona es una propiedad que tienen muchos teléfonos celulares en la actualidad y pueden reconstruir los movimientos específicos de una persona minuto a minuto. No solo en la ciudad, sino también en un edificio en particular...

Las aplicaciones de *software* ofrecen un rango de herramientas para administrar información detallada de todos los aspectos personales de la vida de una persona. Hay aplicaciones para obtener información sobre el Partido Demócrata y el Partido Republicano; aplicaciones para las adicciones a las drogas, al alcohol y al juego; aplicaciones para compartir pedidos de oración; para chequear síntomas de embarazo; aplicaciones para planear un presupuesto; aplicaciones para cada hábito o pasatiempo; aplicaciones para mejorar la vida amorosa. Hay aplicaciones muy populares para comprar y vender casi cualquier cosa y los registros de esas transacciones están accesibles en el teléfono celular de modo indefinido. Hay más de un millón de aplicaciones disponibles en cada una de las dos grandes tiendas de aplicaciones; la frase: "Hay una aplicación para eso" ahora es parte del léxico popular. El usuario de teléfono celular promedio ha instalado 33 aplicaciones, que en conjunto forman un montaje revelador de la vida del usuario.

En 1926, Learned Hands observó (opinión luego citada en Chimel) que una cosa totalmente distinta es registrar los bolsillos de un hombre y usar en su contra lo hallado, que registrar su casa en búsqueda de cualquier cosa que podría llegar a incriminarlo. De todos modos, si sus bolsillos contienen un celular esto último no podría ser aplicado. Por cierto, la requisa de un celular expondría a la autoridad pública mucho más que la búsqueda más exhaustiva realizada en un domicilio: un teléfono celular no solo contiene en formato digital muchos registros sensibles previamente encontrados en la casa; sino que también contiene un gran espectro de información privada nunca encontrada en una casa en ningún formato, al menos que se encuentre el celular.

Vigilancia electrónica aplicada como medio sustitutivo al encierro

Una de las aplicaciones más extendidas de los dispositivos de vigilancia electrónica se registra en materia de encarcelamiento preventivo y ejecución de penas. A raíz de la inocultable situación de abandono en la que se encuentra la estructura edilicia del sistema penitenciario en nuestro país, sumado al fracaso generalizado de los programas de resocialización, se ha ensayado en los últimos tiempos la admisión de las nuevas tecnologías de geolocalización para evitar la privación de la libertad innecesaria y así fomentar en cierta medida la resocialización de las personas detenidas evitando su exclusión del núcleo familiar y social.

En nuestro país, la Resolución Nº 1379/2015 del Ministerio de Justicia y Derechos Humanos, suscripta el 26 de junio de 2015, dispone un programa de asistencia de personas bajo vigilancia electrónica, en consonancia con lo establecido por el artículo 10 del Código Penal y los artículos 32 y 33 de la Ley Nº 24660 (Ley de Ejecución de la Pena Privativa de la Libertad).

Por su parte, la Ley Nº 14296, dictada por el Senado y la Cámara de Diputados de la Provincia de Buenos Aires, ha modificado en 2011 la Ley de Ejecución Penal bonaerense (Ley Nº 12256) para receptar, en sus arts. 19 y siguientes (en especial, el art. 20), el uso de monitoreo electrónico para el arresto domiciliario.

Idéntica factura y finalidad se encuentra en la Ley Nº 8218 dictada por el Senado y la Cámara de Diputados de la provincia de Mendoza.

Existen, por lo demás, distintas iniciativas, proyectos y pruebas piloto en el resto de las provincias que integran la República Argentina para hacer realidad la implementación de esta forma de monitoreo electrónico de las personas detenidas o condenadas.[107]

En la República del Salvador, el Decreto N° 924 (2015) ha regulado el uso de medios de vigilancia electrónica en materia penal. La aplicación de estos medios de vigilancia electrónica está dirigida principalmente a los casos de detención provisional y ejecución de la libertad condicional. Entre los dispositivos electrónicos, se cuentan el empleo

107. Existe una iniciativa de adoptar este sistema de seguimiento en la provincia del Chubut.

de brazaletes, tobilleras o chips que permitan monitorear en tiempo real la ubicación de su portador.

También Colombia ha adoptado mediante la sanción de la Ley N° 1453 (2011) el uso de técnicas de vigilancia electrónica de detención domiciliaria y como sustitutivo de la pena de prisión no mayor a los ocho años.

A esta tendencia se ha sumado la República del Perú, mediante la sanción de la Ley Nº 29499, al modificar artículos del Código Penal (art. 52), de la Ley Procesal Penal y de la de Ejecución Penal para adaptar esta nueva forma de vigilancia electrónica a las personas privadas de su libertad, sujeto a la conformidad del afectado.

Pedido de información a los proveedores de servicio de Internet en el marco del proceso penal

La mayoría de la información de los usuarios de Internet está almacenada en empresas privadas. Frecuentemente, las agencias gubernamentales y los tribunales acuden a las empresas proveedoras de servicio para averiguar la identidad de los usuarios, su historial de contactos y visitas, así como cualquier otro dato personal vinculado con la posible comisión de un delito. Debemos recordar que millones de personas emplean habitualmente Internet para consultar información, leer periódicos, intercambiar información o directamente comunicarse con otros.

Existe una relación virtuosa en muchos casos entre las compañías proveedoras del servicio telemático y los servicios públicos, por ejemplo, el sistema de emergencia 911 requiere de los proveedores del sistema la localización del usuario. Por lo general, en el caso de los sistemas telefónicos digitales, esa ubicación surge de la triangulación de las torres de captación de señales utilizadas por esos dispositivos. En el caso de los teléfonos satelitales, esa función de geolocalización la cumplen los satélites. En principio, esa cooperación no solo resulta necesaria, sino que, además, es beneficiosa para terceros.[108]

En algunos casos, las empresas proveedoras intermediarias de servicios, como Google, AOL, eBay y otras tantas, se han opuesto a brindar información sobre sus clientes. Uno de esos casos fue el de

108. Henderson, Stephen, *op. cit.*, p. 379 y ss.

"Gonzales v. Google Inc.",[109] cuando la empresa proveedora intermediaria de servicios en Internet fue intimada por el gobierno federal a aportar información sensible de sus usuarios. Google trata la información de búsquedas y los métodos de indexación y sus resultados como confidencial. Al mismo tiempo, Google fija políticas de privacidad sobre el uso de este servicio de búsqueda. Cada vez que un usuario realiza una búsqueda determinada genera un registro automático en los servidores, que permite saber cuál es el sitio *web* requerido, la dirección IP, el navegador y el idioma empleado.

En el citado caso "Gonzales v. Google Inc.", la Procuración General de los Estados Unidos de América había requerido *(subpoena)* información sobre los filtros y el bloqueo efectivo de búsquedas realizadas por usuarios de ese servicio relacionadas con la pornografía infantil, en el marco de la *Child On line Protection Act* (COPA, por sus siglas en inglés).[110] De esta manera, el gobierno pretendía restringir las búsquedas en Internet de material vinculado con la pornografía infantil. La postura de Google Inc. fue desde el principio negarse a cumplir con esa requisitoria, basándose en el derecho a la confidencialidad de los usuarios del servicio informático, ya que la calidad de la información solicitada permitía no solo identificar a los usuarios, sino también conocer sus ideas, gustos y preferencias. Cabe aclarar que el presente proceso fue de naturaleza civil, ya que en caso de un proceso penal las autoridades deben demostrar que la información solicitada es relevante para la investigación penal, como aconteció en el proceso seguido contra Scott Peterson por el asesinato de su mujer y su hijo nonato ocurrido a fines de 2002.[111] En definitiva, el tribunal terminó por rechazar el pedido del gobierno.

En la actualidad, la información almacenada por los principales proveedores de servicios en Internet y en otros medios de comunicación permite reconstruir aspectos trascendentales de la vida personal. Por esta razón, se ha vuelto cada más frecuente que las autoridades públicas acudan a esas bases de datos para obtener in-

109. 234 F.R.D. 674; 2006 U.S. Dist. Lexis 13412; 64 Fed. Rev. Serv. 3d (Callaghan) 393; 79 U.S.P.Q. 2D (BNA) 1832, decidido el 17 de marzo de 2006.

110. 47 U.S.C. § 231.

111. Foley, Jayni, "Are Google Searches Private - An Originalist Interpretation of the Fourth Amendment in On line Communication Cases", *Berkeley Technology Law Journal*, Vol. 22, Issue 1, 2007, p. 451.

formación sobre una o varias personas. En especial, ese pedido de información colisiona de manera directa con el derecho a la confidencialidad de los datos y con la expectativa razonable de privacidad en el uso de estas herramientas tecnológicas. A su vez, las empresas proveedoras de estos servicios en la sociedad de la información han sido extremadamente recelosas de la privacidad de sus usuarios, ya que entienden perfectamente que el extendido uso de estos medios de comunicación intersubjetivos ha sido favorecido y promocionado sobre la base del derecho de confidencialidad de sus usuarios. No cabe duda de que la erosión de la expectativa razonable de privacidad en el uso de estos servicios telemáticos traería como lógica consecuencia la falta de confianza del público sobre el resguardo de sus derechos personalísimos, al permitir o autorizar el registro y tratamiento de datos por parte de las autoridades públicas, lo que sellaría el destino de esta moderna forma de comunicación.

En la doctrina constitucional americana, el célebre y citado precedente "Katz v. United States"[112] representó un valladar importante contra el accionar de los poderes públicos al considerar que la interceptación de las comunicaciones telefónicas realizadas desde una cabina telefónica violaban la expectativa razonable de privacidad del afectado. Esta doctrina fue receptada y desarrollada en numerosos casos subsiguientes, aunque la propia Corte Suprema de Justicia de ese país fue ajustando el sentido y alcance del mencionado caso "Katz", por ejemplo, al limitar esa expectativa razonable de privacidad, cuando se trata de indagar sobre los números de abonados con los cuales el sospechoso tuvo contacto, ya que esa información fue obtenida directamente de la compañía telefónica; por lo tanto, los funcionarios policiales no se introdujeron en el área constitucionalmente protegida,[113] o bien en el caso de pedidos de informes bancarios de una persona sospechada de cometer un delito.[114]

De acuerdo con la línea jurisprudencial trazada por los tribunales americanos respecto del sentido y alcance de la doctrina de la "expectativa razonable de privacidad", se han presentado casos en

112. 389 U.S. 347, 1967.

113. "Smith v. Maryland", 442 U.S. 735, 742, 1979.

114. "United States v. Miller", 425 U.S. 435, 1976.

la moderna sociedad de la información en los que se ha discutido, por ejemplo, si la información brindada por el proveedor del servicio de la dirección IP equivale a un "dato sensible" de su usuario. Por ende, esa información caería dentro del derecho a la privacidad. Una primera postura sostiene que esa información sobre la dirección IP de un cliente del servicio en Internet no afecta tal derecho, porque el usuario al suscribir el servicio sabe previamente que su información puede ser comunicada a terceros.[115]

Precisamente, el dilema que encierra la moderna sociedad de la información respecto del sentido y alcance del derecho a la privacidad se vincula con los límites difusos de la expectativa subjetiva de privacidad del usuario del servicio de Internet y el aspecto objetivo de la razonabilidad de esa expectativa.[116] Por ejemplo, cuando un usuario publica u ofrece un comentario en las redes sociales puede entender que esa expresión de libertad se canaliza en el ámbito de un grupo limitado de personas, pero ello puede no ser razonable para el mundo virtual. Si tomamos el mismo ejemplo, pero en este caso la opinión es vertida en su propio domicilio en el curso de una reunión de amigos, esa expectativa de privacidad (confidencialidad) puede ser sostenida de modo legítimo, ya que la posibilidad de trascendencia de esa acción está resguardada de la injerencia de terceros, en especial, de la actividad del propio Estado.

El ámbito de privacidad y la expectativa de confidencialidad consecuente se han ido paulatinamente reduciendo en la moderna sociedad de la información, por los adelantos técnicos que permiten captar señales, transmisiones, datos o imágenes de terceros sin necesidad de provocar una injerencia formal en el ámbito privado del afectado. Esto lo dejó bien claro la Corte Suprema de Justicia americana en el precedente "Dow Chemical Co. v. United States" con el uso de cámaras fotográficas para obtener imágenes de la propiedad del acusado desde un aeroplano.

115. "Guest v. Leis", 255 F. 3d 325, 336 (6th Cir. 2001); "United States v. Kennedy", 81 F. Supp. 2d 1103, 1110 (D. Kan. 2000); "United States v. Hambrick", 55 F. Supp. 2d 504, 508 (W.D. Va. 1999).

116. Etzioni, Amitai, "Eight Nails into Katz's Coffin", *Privacy in a Cyber Age. Policy and Practice*, Palgrave Macmillan, Nueva York, 2015, p. 54 y ss.

¿Qué queda en pie del derecho a la privacidad?

Ha quedado debidamente demostrado que el progreso en materia de tecnología informática en la moderna sociedad ha favorecido como nunca antes la expansión de las relaciones intersubjetivas sin fronteras ni controles. Frente a este lado positivo del asunto, debemos subrayar también, y sin temor a equívocos, que los adelantos técnicos han reducido de manera gradual el ámbito de la privacidad individual.

Existe en el plano internacional una honda preocupación por las actividades de espionaje llevadas adelante por las principales potencias mundiales, que dejan al descubierto la fragilidad de la tutela del derecho a la privacidad. Sin importar que numerosos tratados y pactos internacionales aseguran este derecho básico del individuo, la multiplicidad de operaciones encubiertas consistentes en el almacenamiento, registro y tratamiento de datos sensibles de las personas (interceptación de correos electrónicos y llamadas telefónicas, por caso) confirman que los avances tecnológicos en materia de transmisión de datos han sido puestos al servicio de los poderes públicos para controlar a la población.

En el caso de los Estados Unidos de América, las reformas operadas en materia de espionaje durante las distintas administraciones del Poder Ejecutivo y los escándalos desatados por la utilización del programa Echelon y la revelación de secretos por parte de Snowden han expuesto a la luz pública la gravedad y la intensidad de esta forma de injerencia arbitraria en el ámbito de la privacidad de las personas.[117]

En materia de Derecho Procesal Penal, la cuestión dista de ser sencilla. A la futilidad del concepto de imputado o acusado en el proceso penal, se suma la sospecha cierta de que, en muchos casos, las investigaciones judiciales despliegan su arsenal inquisitorio con mínimos presupuestos o fundamentos, y justifican ese proceder en la alegada complejidad del objeto procesal, en especial en materia de narcotráfico, ciberpornografía o terrorismo. La adopción de medidas probatorias consistente en la interceptación de comunicaciones telefónicas o informáticas, allanamientos de domicilio, registros y secuestro de

117. Severson, Daniel, "American Surveillance of Non-U.S. Persons: Why New Privacy Protections Offer Only Cosmetic Change", *Harvard International Law Journal*, Vol. 56, 2015, p. 465 y ss.

computadoras se incrementan de manera exponencial en el trámite de numerosos procesos penales, siendo, en todo caso, difícil de justificar esa medida judicial desde la perspectiva de los principios de necesidad, idoneidad y proporcionalidad de esta forma de injerencia en el ámbito privado de las personas.[118]

Se discute cuál es el límite de una investigación penal que hace uso de este tipo de herramientas técnicas de infiltración en el ámbito personal, familiar y social de una persona sospechada de haber participado en la comisión de un delito.[119] De la cantidad de datos sensibles almacenados en esa pesquisa, corresponderá que el legislador determine cuáles de esos datos deben ser eliminados de manera inmediata –al no guardar relación de afinidad con la naturaleza de la investigación– y cuáles serán pasibles de ser objeto de almacenamiento y posterior tratamiento.

Íntimamente vinculado con la calidad de sospechoso y el alcance del derecho a la privacidad amparado por los arts. 18 y 19 de la Constitución Nacional, se ha discutido si los extranjeros imputados de delitos graves cometidos en el país o contra sus intereses están abarcados por esa garantía de inviolabilidad del domicilio y los papeles privados. En realidad, esta cuestión fue saldada en sentido negativo para los intereses del extranjero acusado de delito de conspiración para cometer espionaje, en el precedente "Abel v. United States".[120] Sintéticamente, acá se debatió si el secuestro de material incriminante (documentos de identidad falsificados, mensajes codificados) obtenido del allanamiento realizado sin orden judicial en el cuarto de hotel que ocupaba el acusado –quien se encontraba detenido por la autoridad migratoria dentro del proceso de deportación– constituía una infracción a la citada inviolabilidad del domicilio y de los papeles privados.

La Corte Suprema de Justicia norteamericana subrayó que el arresto del sospechoso fue practicado de modo válido bajo el auspicio de la Ley de Deportación, pues los agentes contaron con la respectiva orden de arresto emitida por la autoridad competente. Consecuentemente, el tribunal se ocupó de decidir sobre la validez del registro de la habitación de hotel donde habitaba el acusado y el secuestro de ma-

118. Al respecto, CSJN, P.1666. XLI. R.H. "Peralta Cano", del 3/05/2007, con expresa remisión al dictamen del procurador general; y Fallos: 333:1674 ("Quaranta").

119. Rux, Johannes, *op. cit.*, p. 291; Kemper, Martin, *op. cit.*, p. 109.

120. 362 U.S. 217 (1960).

terial incriminante. Sobre este aspecto, la opinión de la mayoría de los integrantes del tribunal coincidió en que el registro y secuestro habían sido legítimos, al establecer una distinción en el alcance del derecho a la privacidad a partir de la naturaleza administrativa del procedimiento de deportación. En síntesis, al no tratarse de un proceso penal, el registro y secuestro de elementos que comprueban la estadía irregular del acusado en el país receptor en el curso de un proceso de deportación queda excluido del ámbito de aplicación de la Cuarta Enmienda de la Constitución norteamericana. Por lo demás, los documentos de identidad falsificados fueron descubiertos en el trámite del proceso de detención por ingreso ilegal al país, en cuyo caso los funcionarios públicos actuaron de modo legal al secuestrar el material en posesión del acusado ya que se trataba de evidencia que podía ser destruida por el propio interesado. Asimismo, se afirmó que el propietario del hotel había dado su consentimiento para el registro posterior de la habitación ocupada por el acusado, quien, luego de abonar su estadía bajo detención, hizo abandono de ese lugar. Por ende, el secuestro de material probatorio adicional puede ser introducido de modo válido en el proceso penal sustanciado de manera posterior.[121]

A esto se agrega, además, la publicidad de esas medidas judiciales en los medios de comunicación masivos que exponen, en algunos casos, aspectos de la vida personal del sospechoso que no están relacionados directamente con el objeto de la investigación judicial, en especial preferencias, gustos u opiniones que deberían quedar resguardadas del escrutinio público, *in fortiori*, cuando dichos aspectos de la vida personal son relevados por los propios investigadores o responsables del proceso.

A esto último debe sumarse el sentido y alcance del consentimiento prestado por el afectado para la ejecución del allanamiento, registro y secuestro de material informático vinculado con la posible comisión de delitos. Si bien nuestra Corte Suprema de Justicia y los tribunales inferiores han desarrollado criterios para juzgar el alcance del consentimiento prestado por el imputado o sus allegados para legitimar un allanamiento de domicilio realizado sin orden judicial, en los últimos

121. En este sentido, resulta interesante señalar que el secuestro de papeles hallados en el cesto de basura del cuarto de hotel habitado por el acusado fue considerado válido bajo el argumento de que el lugar donde fueron encontrados representaba su voluntad de abandono, con arreglo al precedente "Hester v. United States" 265 U.S. 57, 58.

tiempos, nuestro máximo tribunal ha subrayado que ese proceder vulnera el artículo 18 de la Constitución Nacional.[122]

En igual sentido, se ha expedido la Corte Suprema de Justicia norteamericana en el caso "Georgia v. Randolph",[123] al sostener que el consentimiento prestado por uno de los ocupantes (en este caso su cónyuge) del inmueble para la realización de una pesquisa sin orden judicial, pese a que el interesado, que se encontraba presente en el lugar, había manifestado su negativa al registro en ese mismo momento, torna de irrazonable el procedimiento policial que culminó con el secuestro de droga en el domicilio invadido y que fue utilizado como prueba de cargo en el proceso penal posterior.

El artículo 18 de la Constitución Nacional se refiere al domicilio, correspondencia epistolar y papeles privados como lugares y objetos sobre los que existe una expectativa razonable de confidencialidad y así una garantía de inviolabilidad frente a los registros y secuestros arbitrarios realizados por la autoridad pública. Una interpretación dinámica de esa garantía –aplicada al progreso tecnológico en el campo de las comunicaciones y la información en nuestra moderna sociedad– no puede menos que admitir que las comunicaciones telemáticas, los correos y documentos electrónicos se encuentran necesariamente incluidos en ese listado,[124] en consonancia con las reformas operadas en el Derecho Positivo argentino que extendió, por ejemplo, la tutela penal de la confidencialidad a los correos y documentos electrónicos (arts. 77, 153, 153 *bis*, 155, 157, 157 *bis*, todos ellos del Código Penal). En el Derecho Judicial Comparado, los tribunales constitucionales han subrayado esta relación entre el derecho a la autodeterminación informática (art. 2, párrafo primero en relación con el art. 1, párrafo primero, de la Ley Fundamental alemana) en el campo de la libre comunicación de ideas (art. 10 de ese mismo texto constitucional) que abarca de manera

122. CSJN, V. 208. XXXVI. R. H. "Ventura, V.", del 22/02/2005.

123. 547 U.S. 103, 2006.

124. Carbone, Carlos Alberto, *Grabaciones, escuchas telefónicas y filmaciones como medio de prueba*, Santa Fe, Rubinzal-Culzoni Editores, 2006, p. 207; García González, Javier, "Intervenciones de terceros en el correo electrónico. Especial referencia al ámbito laboral y policial", p. 297 y ss.; Schantz, Peter, *op. cit.*, p. 317; Hauck, Pierre, *op. cit.*, p. 422.

necesaria a los nuevos medios de transmisión de datos.[125] El espíritu tuitivo de esa disposición constitucional tuvo en miras la protección integral de la persona en el ámbito de su privacidad personal, plasmándose el ejercicio del derecho de privacidad en las conductas realizadas en el domicilio, o la expresión de ideas u opiniones vertidas en el papel durante el transcurso de un intercambio epistolar.

En nuestra opinión, el artículo 18 de la Constitución Nacional establece como condición inexcusable la existencia de una orden judicial para llevar a cabo un allanamiento de domicilio,[126] condición que se extiende necesariamente a la persona, correspondencia postal y electrónica, interceptación de comunicaciones telefónicas y telemáticas, contenido de documentos electrónicos. En suma, el consentimiento del afectado, *in fortiori*, cuando se encuentra en calidad de detenido, no puede ser valorado como una renuncia expresa de esta tutela constitucional, siendo en todo caso necesario que las investigaciones de los agentes públicos cuenten con el indispensable control judicial que se traduce en el libramiento de la referida orden de allanamiento. Justamente, en este aspecto, se evidencia con fuerza el necesario control sobre la necesidad, idoneidad y proporcionalidad de esa medida de intervención.[127]

Decíamos que el monitoreo *online* de los dispositivos electrónicos y las comunicaciones entabladas por un sospechoso afectan directamente el artículo 18 de la Constitución Nacional cuando esa medida procesal no ha sido precedida de una orden judicial que permita controlar la existencia de motivos suficientes para adoptar tamaña medida de injerencia en el ámbito personal de los individuos. Su autorización judicial debe estar determinada en un plazo y lugar

125. BVerfGE 2 BvR 2099/2004, decisión del 2/03/2006 (LG Karlsruhe), BVerfG HRRS 2006, Nº 235. Al respecto, Schlegel, Stephan, *op. cit.*, p. 44 y ss.

126. La doctrina nacional mantiene un criterio distinto al admitir la posibilidad del allanamiento del domicilio sin orden judicial basado en el probado y libre consentimiento del afectado, cfr. Binder, Alberto, *Introducción al derecho procesal penal*, 2ª ed., 7ª reimp., Buenos Aires, Ad-Hoc, 2016, p. 189. Sobre el desarrollo de la doctrina judicial nacional, sumado a la interpretación restrictiva del sentido y alcance del consentimiento prestado por el interesado puede verse en Carrió, Alejandro, *Garantías constitucionales en el proceso penal*, 5ª ed., 4ª reimp., Buenos Aires, Hammurabi, 2012, p. 408 y ss., en especial, p. 420; Clariá Olmedo, Jorge, *Derecho procesal penal*, T. II, Santa Fe, Rubinzal-Culzoni, 1998, p. 393 y ss.

127. En este sentido, Maier, Julio, *Derecho Procesal Penal*, T. III, Parte general, Buenos Aires, Editores del Puerto, 2011, p. 188.

determinados, evitándose así una infiltración *sine die* que conduzca a tachar de arbitraria y desproporcional la medida judicial. Sumado a la garantía de inviolabilidad de las comunicaciones personales y al derecho de autodeterminación informática que están en juego de manera prístina en la adopción de este tipo de prueba invasiva, se ha subrayado también que la inviolabilidad del domicilio puede afectarse con este tipo de medidas procesales extremas para el derecho a la privacidad, cuando las autoridades públicas utilizan artefactos electrónicos o sistemas informáticos (por ejemplo, en el caso del *keylogging*, activación remota de cámaras, utilización de micrófonos o empleo de sensores infrarrojos) que permiten acceder al ámbito de privacidad del domicilio amparado por el citado artículo 18 de la Constitución Nacional.[128]

En síntesis, se hace imperioso regular de manera expresa las hipótesis que habilitan a los jueces a la adopción de medidas procesales de naturaleza probatoria que tengan por objeto la interceptación de comunicaciones telemáticas, su registro, almacenamiento y tratamiento, siendo en todo caso necesario sujetar esas medidas a un plazo temporal y a la comprobación de una causa probable de la comisión de un delito. Es injustificado fundamentar tales medidas de infiltración informática en apreciaciones subjetivas de los investigadores o meros indicios. El juez deberá fundamentar en el caso concreto la necesidad de esa medida procesal cuando fuese imposible por otros medios comprobar la materialidad del hecho pesquisado, la idoneidad de esa medida por encima de otra fuente de prueba y, por último, la proporcionalidad de su ejecución traducida en la fijación de un plazo temporal, lugar determinado y respecto de personas expresamente individualizadas.

Conclusiones

En la sociedad de la información, el progreso tecnológico en materia de comunicación y el desarrollo de sistemas y programas de detección, registro, almacenamiento y tratamiento de datos sensi-

128. Rux, Johannes, *op. cit.*, p. 292 y ss., p. 295; Schantz, Peter, *op. cit.*, p. 313 y ss. De otra postura, Hauck, Pierre, *op. cit.*, p. 423, al sostener que el monitoreo *online* menoscaba la confidencialidad de la comunicación (información) del afectado, pero no la privacidad del domicilio en un sentido espacial.

bles han extendido de manera peligrosa la posibilidad de la injerencia del Estado en desmedro del ámbito cada vez más reducido de la esfera de la privacidad individual. Ello significa que la capacidad de intervención de las autoridades públicas en el ámbito privado de las personas se ha incrementado de manera exponencial al calor del uso global de esta forma de tecnología. La dependencia creciente e irreversible de nuestra sociedad respecto de los sistemas informáticos nos expone de manera involuntaria al peligro de infiltraciones tanto ilícitas como lícitas (bajo control judicial) fruto del deslinde cada vez más etéreo de la calidad de imputado en el proceso penal.

El concepto de privacidad elaborado y desarrollado durante décadas a través de la doctrina y la jurisprudencia atraviesa en la actualidad un período de crisis como consecuencia de la irrupción de los medios informáticos en la moderna sociedad tecnológica. La expectativa de privacidad en las redes telemáticas se ha contraído de manera grave por las posibilidades crecientes de injerencias extrañas. Lo que una sociedad entendía hace varias décadas atrás como una expectativa razonable de privacidad, ha quedado en cierta medida desactualizado gracias al avance de la tecnología y las posibilidades crecientes de comunicación intersubjetiva entre los integrantes de la sociedad. El almacenamiento masivo de datos, registros y documentos por parte de las empresas prestadoras del servicio de Internet y el interés desbordante de los gobiernos por esa *big data* acorrala de manera subrepticia el derecho de privacidad de las personas. El concepto de privacidad ya no puede ser asimilado a lo que un individuo puede o no hacer dentro de su domicilio o al derecho de exclusión de terceros. En la actualidad, la interactuación de las personas en las redes telemáticas ofrece al mismo tiempo un desafío y una necesidad imperiosa de extender ese concepto a las relaciones intersubjetivas proyectadas en grupos de discusión, foros o *chat room*. La privacidad no debería quedar anclada a un lugar determinado, por ejemplo, en el sentido ya clásico, nuestra morada o domicilio, sino que los dispositivos o artefactos electrónicos, la extensión de las formas de comunicación y el registro de nuestro comportamiento diario, mediante sistemas avanzados de geolocalización, abren una ventana técnica que hace posible que nuestra intimidad pueda ser amenazada o menoscabada directamente mediante la aplicación de técnicas de seguimiento de nuestra huella informática.

La masiva tecnificación de nuestra sociedad ofrece incontables beneficios, al mismo tiempo que incrementa el riesgo de poder ejercer un mayor control por parte de terceros o gobiernos sobre nuestros hábitos sociales, económicos, de consumo, todo lo cual permite el tratamiento de esa información acumulada para utilizarla con fines ajenos a nuestras expectativas de privacidad.[129]

La aplicación de medios técnicos para indagar sobre la posible comisión de un delito mediante la invasión de la privacidad –sin necesidad de injerencia física en el domicilio del afectado– ha sido traída a la palestra, por ejemplo, al utilizarse un escáner térmico para determinar la existencia de una plantación de marihuana que demandaba condiciones ambientales adecuadas que solo podían ser ofrecidas gracias al uso de lámparas especiales que incrementaban el consumo promedio de energía.[130] En una ajustada mayoría, el máximo tribunal norteamericano se inclinó por tachar de irrazonable ese registro del domicilio del afectado, de acuerdo con el voto preopinante del juez Scalia, en función del uso exclusivo de esos aparatos en poder de los funcionarios públicos y que el resultado del registro realizado en el domicilio, mediante el uso de esa tecnología, solo era posible mediante la intromisión física en ese ámbito. De esta manera, el voto mayoritario puso el énfasis en que existía una expectativa razonable de privacidad por parte del acusado, que el registro térmico de su domicilio se llevó a cabo con medios no habituales que permitían el escaneo del interior del domicilio y, por último, que el registro térmico posibilitó detectar el funcionamiento de una presunta plantación de marihuana, cuyo descubrimiento no podría haber sido posible, salvo mediante la intrusión física de los funcionarios públicos.

129. Spencer, Shaun, "Reasonable Expectations and the Erosion of Privacy", *Washington Law Review*, Vol. 79, 2002, p. 843 y ss. El concepto de expectativa razonable de privacidad se encuentra en crisis desde hace tiempo en razón de la dificultad de determinar con precisión qué se entiende por razonable para una sociedad en un momento determinado. La propia doctrina judicial norteamericana expone esa dificultad al distinguir distintas esferas de actuación, por ejemplo, la pública y la privada, incluso reduciendo esa expectativa razonable de privacidad frente a registros y secuestros sin orden judicial practicados por particulares en el marco de la sustanciación de un sumario administrativo o por parte del empleador respecto de sus dependientes.

130. "Kyllo v. United States", 533 U.S. 27, 2001. Al respecto, Hardee, Sarilyn, "Why the United States Supreme Court's Rule in 'Kyllo v. United States' Is Not the Final Word on the Constitutionality of Thermal Imaging", *Campbell Law Review*, Vol. 24, 2001, p. 53 y ss.

En este aspecto, es menester regular de manera exhaustiva en las leyes procesales penales –en función del espíritu liberal que guio la pluma que redactó los arts. 18 y 19 de la Constitución Nacional–, las condiciones de posibilidad de este tipo de injerencias extremas en el círculo de las acciones privadas por parte de las autoridades públicas. En particular, es necesario determinar *a priori* la calidad de los datos sensibles que deben quedar extramuros del objeto de una investigación penal y el deber de borrar la información que puede afectar el derecho a la privacidad personal y familiar. Las posibilidades técnicas que nos ofrecen hoy en día la ciencia tecnológica y el progreso alcanzado en el campo de la transmisión de datos no deben eclipsar la necesidad de fortalecer la tutela de los derechos fundamentales de la persona, *in fortiori*, en el Derecho Procesal Penal. Que sea viable técnicamente la interceptación de conversaciones personales mediante el uso de satélites, *drones*, computadoras o artefactos de escucha teledirigidos no habilita ni justifica su uso indiscriminado por fuera del control judicial. En la actualidad, podemos presenciar habitualmente que el acceso indebido a datos sensibles de terceros y su posterior publicación o difusión se han transformado en moneda corriente. Contra esa ignominiosa tendencia de atentar contra la privacidad personal solo cabe oponer el respeto estricto de los derechos básicos de las personas y, en el caso del proceso penal, extremar los recaudos de control judicial sobre la investigación fiscal basada en la necesidad, idoneidad y proporcionalidad de esas medidas de interceptación, satisfaciéndose así el papel de contralor natural del juez en el ejercicio razonable del poder público en el marco de un Estado de derecho.

Bibliografía

ARENAS RAMIRO, Mónica, "La protección de los datos personales en los países de la Comunidad Europea", *Revista Jurídica de Castilla y León*, N° 16, septiembre de 2008.

ARZT, Gunther; WEBER, Ulrich; HEINRICH, Bernd; HILGENDORF, Eric, *Strafrecht*. Besonderer Teil, 2. Aufl., Gieseking, Bielefeld, 2009.

BALKIN, Jack, "The Constitution in the National Surveillance State", *Minnesota Law Review*, Vol. 93, Nº 17-18, 2008.

BAUMAN, Zygmunt, "After Snowden: Rethinking the Impact of Surveillance", *International Political Sociology*, Vol. 8, 2014.

BINDER, Alberto, *Introducción al Derecho Procesal Penal*, 2ª ed., 7ª reimp., Buenos Aires, Ad-Hoc, 2016.

BLITZ, Marc Jonathan, "The Fourth Amendment Future of Public Surveillance: Remote Recording and other Searches in Public Space", *American University Law Review*, Vol. 63, N° 1, 2013.

BROWN, Jeremy, "Pan, Tilt, Zoom: Regulating the Use of Video Surveillance of Public Places", *Berkeley Technology Law Journal*, Vol. 23, 2008.

BUERMEYER, Ulf, "Die On line-Durchsuchung. Technischer Hintergrund des verdeckten hoheitlichen Zugriffs auf Computersysteme", HRRS, Heft 4/2007.

CARBONE, Carlos Alberto, *Grabaciones, escuchas telefónicas y filmaciones como medio de prueba*, Santa Fe, Rubinzal-Culzoni Editores, 2006.

CARRIÓ, Alejandro, *Garantías constitucionales en el proceso penal*, 5ª ed., 4ª reimp., Buenos Aires, Hammurabi, 2012.

CLANCY, Thomas K., "What Does The Fourth Amendment Protect: Property, Privacy, or Security", *Wake Forest Law Review*, Vol. 33 (2009).

CLARIÁ OLMEDO, Jorge, *Derecho Procesal Penal*, T. II, Santa Fe, Rubinzal-Culzoni, 1998.

CORTÉS BECHIARELLI, Emilio, "El insoportable anacronismo de los abusos policiales en el marco de la instrucción criminal a la luz de las nuevas técnicas de investigación", en González Cussac, José Luis y Cuerda Arnau, María Luisa (dirs.), Fernández Hernández, Antonio (coord.), *Nuevas amenazas a la Seguridad Nacional. Terrorismo, criminalidad organizada y tecnologías de la información y la comunicación*, Valencia, Tirant Lo Blanch, 2013.

CRAMPTON, Jeremy, "Collect it all: National Security, Big Data and Governance", *GeoJournal*, agosto de 2015 (referencia: DOI 10.1007/s10708-014-9598).

DELMAS-MARTY, Mireille (dir.), *Procesos penales de Europa (Alemania, Inglaterra y País de Gales, Bélgica, Francia, Italia)*, Zaragoza, Edijus, 2000.

DÍEZ RIPOLLÉS, José Luis, "De la sociedad del riesgo a la seguridad ciudadana: Un debate desenfocado", *RECPC* 07-01, 2005.

DWORK, Cynthia; MULLIGAN, Deirdre, "It's not privacy, and it's not fair", *Stanford Law Review On line*, Vol. 66, 3 de septiembre de 2013.

ETZIONI, Amitai, "Eight Nails into Katz's Coffin", *Privacy in a Cyber Age. Policy and Practice*, Nueva York, Palgrave Macmillan, 2015.

FLORES PRADA, Ignacio, "Prevención y solución de conflictos internacionales de jurisdicción en materia de ciberdelincuencia", *Revista Electrónica de Ciencia Penal y Criminología*, N° 17, 2015.

FOLEY, Jayni, "Are Google Searches Private - An Originalist Interpretation of the Fourth Amendment in On line Communication Cases", *Berkeley Technology Law Journal*, Vol. 22, Issue 1, 2007.

GARCÍA GONZÁLEZ, Javier, "Intervenciones de terceros en el correo electrónico. Especial referencia al ámbito laboral y policial", *El cibercrimen. Nuevos retos jurídico-penales, nuevas respuestas político-criminales*, Estudios de Derecho Penal y Criminología, dirigidos por Carlos María Romeo Casabona, Vol. Nº 78, Granada, Comares, 2006.

GERADIN, Damien; KUSCHEWSKY, Monika, "Competition Law and Personal Data: Preliminary Thoughts on a Complex Issue". Disponible en: http://ssrn.com.abstract=2216088.

GERHOLD, Sönke, *Das System des Opferschutzes im Bereich des Cyber- und Internetstalking*, Baden-Baden, Nomos, 2010.

GONZÁLEZ CUSSAC, José Luis, "Estrategias legales frente a las ciberamenazas", *Cuadernos de Estrategia*, Nº 149, 2011.

HARDEE, Sarilyn, "Why the United States Supreme Court's Rule in 'Kyllo v. United States' Is Not the Final Word on the Constitutionality of Thermal Imaging", *Campbell Law Review*, Vol. 24, 2001.

HAUCK, Pierre, *Heimliche Strafverfolgung und Schutz der Privatheit*, Veröffentlichungen zum Verfahrensrecht, Bd. 102, Mohr Siebeck, Tübingen, 2014.

HENDERSON, Stephen, "Learning from All Fifty States. How to Apply the Fourth Amendment and Its State Analogs to Unreasonable Search", *Catholic University Law Review*, Vol. 55, 2006.

HILGENDORF, Eric, "Aktuelle Fragen des materiellen Computerund Internet-strafrechts im Spiegel neuerer Gesamtdarstellungen", *Zeitschrift für die gesamte Strafrechtswissenschaft* (ZStW), Vol. 118, N° 1, 2006.

HILGENDORF, Eric; FRANK, Thomas y VALERIUS, Brian, *Computer-und Internetstrafrecht*, Berlín, Springer, 2005.

KEMPER, Martin, "Anforderung und Inhalt der On line Durchsuchung bei der Verfolgung von Straftaten", *Zeitschrift für Rechtspolitik* (ZRP), 40. Jahrg., N° 4, 2007.

KLESCZEWSKI, Diethelm, "Stratataufklärung im Internet-Technische Möglichkeiten und rechtliche Grenzen von strafprozessualen Ermittlungseingriffen im Internet", *Zeitschrift für die gesamte Strafrechtswissenschaft* (ZStW), Vol. 123, N° 4, 2012.

KOCHHEIM, Dieter, *Cybercrime und Strafrecht in der Informations- und Kommunikationstechnik*, Beck, Múnich, 2015.

LAWNER, Kevin, "Post-Sept. 11th International Surveillance Activity- A Failure of Intelligence: The Echelon Interception System & the Fundamental Right to Privacy in Europe", *Pace International Law Review*, Vol. 14, N° 2, 2002.

LEMAN-LANGLOIS, Stéphane, "Questions au sujet de la cybercriminalité, le crime comme moyen de contrôle du cyberespace commercial", *Criminologie*, Vol. 39, N° 1, 2006.

MAIER, Julio, *Derecho Procesal Penal*, T. III, Parte general, Buenos Aires, Editores del Puerto, 2011.

MANES, Jonathan, "On line Service Providers and Surveillance Law Transparency", *The Yale Law Journal Forum*, 2016, pp. 343-358.

MARTÍNEZ MARTÍNEZ, Ricard, "Los ficheros de datos y archivos de imágenes policiales en la legislación italiana. Análisis de las resoluciones dictadas por el garante italiano para la protección de datos personales", *Revista Española de Derecho Constitucional*, Año 20, N° 60, septiembre-diciembre de 2000.

MITSCH, Wolfgang, *Medienstrafrecht*, Berlín, Springer, 2012.

MUÑOZ CONDE, Francisco, *Valoración de las grabaciones audiovisuales en el proceso penal*, Buenos Aires, Hammurabi, 2004.

NAKASHIMA, Ellen, "After 11 Years, a Curtain Is Lifted on a Secret FBI Demand for a Target's Data", *Washington Post*, 30/11/2015. Disponible en: https://www.washingtonpost.com

NEUBACHER, Frank, "An den Grenzen des Strafrechts-Stalking, Graffiti, Weisungsverstöße", *Zeitschrift für die gesamte Strafrechtswissenschaft*, Vol. 118, 2006, Heft 4.

PURICELLI, José Luis, "Informática y delito", *Derecho Penal y Derecho Procesal Penal*. Homenaje a Carlos Alberto Contreras Gómez, Buenos Aires, Abeledo-Perrot, 1997.

ROMEO CASABONA, Carlos María, "De los delitos informáticos al cibercrimen. Una aproximación conceptual y político-criminal", *El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales*, Estudios de Derecho Penal y Criminología, dirigidos por Carlos María Romeo Casabona, Vol. Nº 78, Granada, Comares, 2006.

ROXIN, Claus, "Libertad de autoincriminación y protección de la persona del imputado en la jurisprudencia alemana reciente", *Estudios sobre Justicia Penal*, Homenaje al profesor Julio B. J. Maier, Buenos Aires, Editores del Puerto, 2005.

ROXIN, Claus; ARZT, Gunther y TIEDEMANN, Klaus, *Introducción al Derecho Penal y al Derecho Penal Procesal*, Barcelona, Ariel Derecho, 1989.

RUX, Johannes, "Ausforschung privater Rechner durch die Polizeiund Sicherheitsbehörden", *Juristenzeitung* (JZ), 62. Jahrg, Nº 6, 2007.

SCHANTZ, Peter, "Verfassungsrechtliche Probleme von 'On line-Durchsuchung'", *Kritische Vierteljahresschrift für Gesetzgebung und Rechtswissenschaft* (KritV), Vol. 90, N° 3, 2007.

SCHLEGEL, Stephan, "Beschlagnahme von E-Mail-Verkehr beim Provider", HRRS, Heft 2/2007.

SCHMÖLZER, Gabriele, "Straftaten im Internet: eine materiell rechtliche Betrachtung", *Zeitschrift für die gesamte Strafrechtswissenschaft* (ZStW), Vol. 123, Heft 4, 2012.

SCHUH, Daniel, *Computerstrafrecht im Rechtsvergleich - Deutschland, Österreich, Schweiz*, Schriften zum Strafrecht, Heft 228, Berlín, Duncker & Humblot, 2012.

SETTY, Sudha, "Surveillance, Secrecy, and the Search for Meaningful Accountability", *Stanford Journal of International Law*, Vol. 16, 2015.

SEVERSON, Daniel, "American Surveillance of Non-U.S. Persons: Why New Privacy Protections Offer Only Cosmetic Change", *Harvard International Law Journal*, Vol. 56, 2015.

SIEBER, Ulrich, *Straftaten und Strafverfolgung im Internet*, Gutachten C zum 69. Deutschen Juristentag, Beck, Múnich, 2012.

SLOBOGIN, Christopher; SCHUMACHER, Joseph, "Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at 'Understandings Recognized and Permitted by Society'", *Duke Law Journal*, Vol. 42, N° 4, 1993.

SPENCER, Shaun, "Reasonable Expectations and the Erosion of Privacy", *Washington Law Review*, Vol. 79, 2002.

STEWART, Potter, "The Road to 'Mapp v. Ohio' and beyond: The Origins, Development and Future of the Exclusionary Rule in Search-and-Seizure Cases", *Columbia Law Review*, Vol. 83, N° 6, octubre de 1983.

VALERIUS, Brian, "Ermittlungsmaßnahmen im Internet", *Juristische Rundschau* (JR), Heft 7, 2007.

WOHLWEND, Sebastian, "Die Durchsuchung, gerade bei Dritten nach § 103 Abs. 1 S. 1 StPO", HRRS, Heft 11/2015.

WRIGHT, Steve, "The Echelon Trail: An Illegal Vision", *Surveillance and Society*, Vol. 2/3, septiembre de 2002.

Responsabilidad penal de la inteligencia artificial. Hacia un paradigma de singularidad tecnológica

Eduardo Aníbal Aguayo*

Introducción

Asistimos con clásica lentitud a observar, sin herramientas clarificadoras para deconstruir el fenómeno de eclosión de una nueva realidad caracterizada por el desplazamiento antropocéntrico, un escenario revolucionario que avanza y se desarrolla con la potencia incontenible de la evolución del descubrimiento.

La aplicación de nuevas tecnologías provenientes del desarrollo de la información y comunicación, en el ámbito de la hiperconectividad de la *web*, de "Internet", ha despertado campos de aplicación para la inteligencia artificial, que ciertamente han modificado parte sustancial de nuestra realidad, con innegable impacto en la conciencia sobre el medio en el que se desenvuelven las relaciones interpersonales. La circunstancia de que la tecnología opere como instancias que conectan masivamente a las personas, a niveles singulares y así también niveles iterativos, ha provocado cierta interpelación de la trama social y la configuración de la realidad de quienes nacimos antes de la expansión de la *web*, trama que así redefinida en nada asombra a los que la nación digital abraza con naturalidad.

* Abogado recibido en la Facultad de Derecho de la Universidad de Buenos Aires. Especialista en Derecho Penal por la Facultad de Derecho de la Universidad Austral, y Doctorando en Derecho Penal y Ciencias Penales por la Facultad de Ciencias Jurídicas de la Universidad del Salvador. Prosecretario Letrado de la Defensoría General de la Nación y Defensor Público Coadyuvante desde 2014.

La vida como se la conocía sufrió un giro radical. Asistimos a una revolución digital ante la aparición de tecnologías disruptivas de la información y comunicación.

Este giro no ha concluido y parte de aquella potencia incontenible del avance tecnológico exige dejar nuestro rol de observadores pacientes y adelantarnos a todo aquello que ha pronosticado históricamente la ficción sobre los logros de la ciencia.

Se avecinan tiempos en los que los desarrollos tecnológicos de la era digital atravesarán horizontalmente y radicalmente numerosos aspectos de la estructura de la sociedad a niveles filosófico, cultural, educativo, económico, sanitario, etc. Estas transformaciones dan lugar hoy a los riesgos inherentes y la criminalidad asociada, con una tendencia a profundizarse a pasos agigantados.

Como sistema de reglas destinado a contemplar las conductas lesivas para el conjunto social y reprochar aquellas que afectan una vida plena, el derecho en general y el penal en particular deberán contener y asignarse también el objetivo de contemplar las conductas que afecten la sustentabilidad de la vida en esta nueva realidad dinámica y de constante transformación.

Desarrollo tecnológico

Tiempo antes de su muerte, Stephen Hawking advirtió, junto a Elon Musk y Bill Gates, sobre los riesgos de la inteligencia artificial (IA). Se trataría del evento más grande de la historia humana, pero según el científico, podría ser el último.[1] En una carta presentada a la Conferencia Conjunta Internacional celebrada en Buenos Aires, en julio de 2015, con la presencia de más de 1200 investigadores, indicó que la inteligencia artificial podría ser más peligrosa incluso que las armas nucleares.

En 2016, el Parlamento Europeo emitió una resolución con recomendaciones dirigidas a la comisión sobre normas de derecho civil

1. Stephen Hawking: "Transcendence looks at the implications of artificial intelligence, but are we taking AI seriously enough?", artículo de opinión publicado en *The Independent*, 1° de mayo de 2014, escrito junto con los científicos Stuart Russell, Max Tegmark y Frank Wilczek. Disponible en: https://www.independent.co.uk/news/science/stephen-hawking-transcendence-looks-at-the-implications-of-artificial-intelligence-but-are-we-taking-9313474.html

sobre robótica.[2] Le asignó importancia vital al fenómeno transformador de las nuevas tecnologías, donde robots, *bots*, androides y demás sistemas y formas concebidas como entes dotados de inteligencia artificial se encuentran en el centro de la escena. Destacó la necesidad de ponderar las consecuencias jurídicas y éticas en este campo revolucionario de innovación.

Se trató el potencial de las nuevas tecnologías para transformar el modo de vida, las relaciones de trabajo y con ello la estructura social y aspectos fundacionales y existenciales del ser humano. Observaron la firme necesidad de orientar el desarrollo tecnológico de la revolución digital hacia un horizonte más justo y equitativo para la sociedad.

Se presenta así, entiendo, un objetivo reparador de las fracturas de clase producto de la exclusión y desigualdad, contrario a la tendencia de concentración de poder y riqueza en minorías con acceso a los beneficios en la materia. Los desarrollos deberán tener como principios orientadores, la seguridad y ética en la innovación, junto con la responsabilidad jurídica de lo producido.

El aumento de sistemas diseñados para adoptar decisiones autónomas, basadas en algoritmos de aprendizaje profundo, prevén y alertan sobre la necesidad de constituir cuerpos éticos, códigos de conducta, códigos deontológicos, licencias para desarrolladores y usuarios, con el objeto de neutralizar los riesgos en este campo, incluso bajo principios tales como el de precaución –concebido en derecho internacional del medioambiente–.

Los sistemas autónomos, bajo el paradigma de la inteligencia artificial, permean y se expanden en todos los campos de la ciencia, información y comunicación.

En este punto debo advertir que la idea de la inteligencia artificial bajo rasgos antropomórficos resulta parcial, para decirlo amablemente, pues la tecnología se expande no sólo en la descripción intuitiva que nos acerca al Robot[3] (concebido con esas características por la influencia de Asimov en su vasta literatura), sino también a todas las herramientas y plataformas tecnológicas que operan nuestro presente.

2. Texto aprobado con fecha 16 de febrero de 2017 –P8_TA(2017)0051–.

3. Término acuñado por Karel Čapek, dramaturgo checo que estrenó la obra *R.U.R.* en 1921 (*Rossumovi univerzální roboti*, en inglés *Rossum's Universal Robots*).

Desde predictores de palabras en dispositivos de telefonía celular, asistentes virtuales como Siri, sistemas de respuesta en la *web* de diversas empresas u organismos, traductores de texto, sistema de identificadores de personas en imágenes, sistemas de navegación automática en transportes autónomos, sistema de reconocimiento de objetos, sistemas de buscadores en línea, hasta programas destinados a poner a prueba las capacidades de procesamiento de información y adaptación, tales como Watson de IBM (aplicado a negocios, tales como bancos, hospitales, comercios y entidades educativas), Deep Blue y AlphaGo, que con sus diferencias pusieron en evidencia la distancia de procesamiento entre la biología humana y el entramado profundo de las redes de inteligencia artificiales; vemos que toda la tecnología de hoy se encuentra atravesada por los avances en los sistemas caracterizados por su autonomía funcional.

Los sistemas *deep learning* o de aprendizaje profundo, resultan ser la base de los desarrollos actuales. Se trata de sistemas de cómputo capaces de aprender a partir de la experiencia, inspirados en principios de funcionamiento del cerebro humano. Las redes neuronales artificiales son esquemas de procesamiento computacional que emulan los niveles o capas responsables de precisar el pensamiento, identificar patrones abstractos y tamizar de manera escalonada hasta las conclusiones derivadas de este conjunto.

El año pasado se dio a conocer un caso ejemplo de aprendizaje profundo: AlphaGoZero. Primeramente el sistema AlphaGo –predecesor del Zero–, desarrollado por Google DeepMind, venció en el juego de tablero estratégico de origen chino llamado Go, al campeón mundial Lee Sedol. Este programa fue desarrollado con la carga de numerosa información relativa a partidas de referencia. Se calcula que se necesitaron más de 30 millones de partidas y meses de entrenamiento para que el sistema se enfrente al Surcoreano campeón del mundo.

Con la puesta en funcionamiento de AlphaGoZero, quedó en evidencia la potencialidad del desarrollo de la tecnología de aprendizaje profundo. Mientras el primer sistema fue instruido con partidas de jugadores expertos y meses de preparación, el nuevo programa fue instruido sólo con las reglas del juego. A partir de ahí comenzó a entrenarse solo. Desde la empresa aseguraron que a las 3 horas de haber comenzado el sistema ya tenía nociones básicas del juego Go, realizaba

jugadas que no tenían en consideración el medio juego y el final. A las 19 horas modificó la tendencia de capturar piezas sin tener en vista el medio juego y comenzó a realizar jugadas con la clara finalidad de dominar el territorio a largo plazo. A las 70 horas tenía un nivel superior al humano, con miras en el medio juego y final. Se concluyó que este diseño, denominado "aprendizaje profundo por refuerzo", trajo un avance en la materia muy valioso. El Go, a diferencia del ajedrez, plantea aspectos estratégicos e intuitivos más allá de la necesidad de la potencia de cálculo, cuyos aspectos de programación comienzan a aparecer con tecnologías que se estructuran a partir de las decisiones autónomas basadas en redes de procesamiento escalonado o neuronal.

AlphaGoZero derrotó a AlphaGo –que había destronado al campeón Lee Sedol– en un torneo de cien partidas: cien a cero.

Aquí hay dos cuestiones relevantes para destacar. Los propios desarrolladores de AlphaGoZero, confesaron la imposibilidad de conocer la etiología de las "decisiones de juego" del sistema, surgiendo un problema claro de trazabilidad de la decisión, por la propia estructuración de las capas algorítmicas, escalonadas o neuronales. Si sólo se lo instruyó sobre las reglas de juego y no se actuó por referencia ni asociación, pareciera que las decisiones del sistema se originan de manera genuina en un segmento libre de influencias.

Pero también se presentan otros aspectos que pueden interferir en el conocimiento del proceso de decisión de los sistemas autónomos, que tienen que ver con el secreto comercial de ciertos desarrolladores y la cerrazón de los códigos fuente.

Tal es el caso de Eric Loomis en Wisconsin, quien fue condenado a seis años de prisión, en parte, porque el juez de la sentencia tomó en consideración la evaluación de riesgo de reincidencia que realizó el programa Compas de la firma Northpointe Inc.

El caso, conocido como "Loomis v. Wisconsin", se basó en un planteo ante la Corte Suprema de los Estados Unidos para anular el fallo de la Corte Suprema de Wisconsin, que rechazó la impugnación del uso por parte de ese Estado de un *software* de evaluación de riesgo de código fuente cerrado o desconocido. La defensa de Loomis planteó que el uso de dicho *software* en la sentencia viola el derecho del acusado al debido proceso porque evita que el acusado impugne la validez científica y la precisión de dicha prueba. La crítica también se alzó en función de

que el sistema viola los derechos al debido proceso al tener en cuenta el género y la raza, y arrojar en función de ellos estadísticas más disvaliosas para los afroamericanos. El asunto quedó sin definición al negarse la Suprema Corte a tratarlo.

Ya sea por cuestiones de secreto comercial o por la naturaleza propia de la tecnología *deep learning* o aprendizaje profundo, mediante algoritmos y redes neuronales de trabajo en capas o forma escalonada, lo cierto es que existe una necesidad ineludible de tener el conocimiento y control sobre los procesos de decisión, la base en función a la cual se gestan y cómo es toda la trama o cadena de procesos a través de los cuales se arriba a una conclusión o decisión por parte del sistema autónomo.

La opacidad de esta tecnología en este punto es conocida como "algoritmo de caja negra", que es básicamente aquel en el que el usuario no puede ver la forma interna de funcionamiento. Este aspecto recibe una fuerte crítica vinculada a que cualquier desarrollo o inteligencia que tenga injerencia en la vida humana, debe tener trazabilidad algorítmica, entendida como la aptitud de reconstruir la historia, la utilización o la localización de un producto por medio de identificaciones registradas. Se trata en esencia de conocer la etiología de proceso decisional del sistema autónomo.

Más adelante veremos si los avances se dirigen hacia ese horizonte o si por el contrario agudizan aún más las dificultades para conocer y controlar esta tecnología. Basta decir ahora que la mayoría de estos múltiples desarrollos han pasado desapercibidos. Lo claro es que abundan los ejemplos que podrían llamar nuestra atención y hasta provocar cierto escepticismo sobre su ocurrencia real.

Este año se conoció que un subsistema de Google, llamado Neural Machine Translation, creado bajo la tecnología de *deep learning* con el objetivo de realizar traducciones más precisas, fue capaz de realizar traducciones entre idiomas respecto de los cuales no había sido instruido.

El año pasado, la Universidad Libre de Bruselas presentó un trabajo en el cual dio a conocer sus conclusiones sobre sistemas autónomos en robots que les permitirán modificar su forma, tamaño y funciones, repararse o reemplazar partes dañadas.

El conglomerado de Facebook creó un sistema originariamente pensado para entablar negociaciones, que consistía en la interacción de dos agentes virtuales. Luego de analizar el funcionamiento se descubrió que

el programa había desarrollado su propio lenguaje, por lo que una vez advertido el patrón de interacción entre los agentes, apagaron el sistema.

Si estos ejemplos no asombran, el caso de Tokio sí debe hacerlo. En las últimas elecciones para la alcaldía de Tama, un distrito de aquella ciudad, la empresa Softbank de Tetsuzo Matsumoto postuló al Robot Michihito Matsuda como alcalde. Según la ley local, un robot no puede ser electo, pero eso no impidió que la candidatura se promocionase con la imagen del androide, a pesar de figurar una persona física en el registro electoral. La promesa de campaña bregaba por oportunidades justas y equilibradas para todos y que como alcalde, el robot analizaría las peticiones, los pros y los contras antes de presentarlas a los representantes del consejo. Además, se prometía contar con un sistema de procesamiento que permitiría encontrar la mejor solución cuando surgieran conflictos, receptar los deseos de los ciudadanos y actuar en función de esas preferencias.

La candidatura testimonial del androide obtuvo el tercer puesto, a solo cuatrocientos votos del segundo puesto, por lo que quedó fuera de la segunda vuelta de los comicios.

Estas tecnologías arrojan también señales de alerta no tan positivas como las reseñadas, que son precisamente las que luego retomaré cuando precise el enfoque, al analizar las implicancias en determinados aspectos de criminalidad en la era digital.

A modo ilustrativo, en 2014 un bot llamado "Random Shopper", programado para operar online y realizar *trading* aleatorio, con una posición semanal de 100 *bitcoins* –moneda virtual–, fue confiscado luego de que decidiera adquirir en la *deep web*, un pasaporte húngaro y dosis de la droga metilendioxi-metanfetamina, más conocida como éxtasis.

En 2016, Microsoft lanzó un bot dotado de inteligencia artificial, cuyo objetivo era mantener conversaciones vía Twitter. La aplicación contaba con un perfil propio llamado Tay. El lanzamiento se produjo el 23 de marzo; la aplicación comenzó a funcionar con comentarios y respuestas aceptables en su interacción. En el lapso de 24 horas se volvió antisemita y racista y fue calificada de nazi por sus tuits.

Ese mismo año un técnico de una planta Volkswagen murió luego de que un robot automatizado de la cadena de montaje lo tomase del pecho y lo aplastase contra una placa metálica.

En materia de transportes autónomos, se registraron accidentes tanto en la firma Ford, Tesla, General Motors, como en Uber, donde se hizo público un video que luego de un pormenorizado análisis, derivó en la conclusión de que el accidente, en el que murió una mujer que cruzaba la calle, debió haber sido evitado por la detección previa de los sensores del vehículo.

Más alarmante que estos casos de incierta etiología, es aquel que envuelve a la temática de los llamados "Robots Asesinos", cuya campaña para desarticular su proliferación se encuentra promovida por Richard Moyes, cofundador de la campaña internacional para abolir las armas nucleares ganadora del Premio Nobel de la Paz en 2017.

En abril de este año, 2018, la Organización de las Naciones Unidas abrió una ronda de conversaciones sobre el desarrollo de máquinas de matar autónomas, diseñadas y producidas con fines bélicos, en el marco de la Convención sobre Armas Convencionales, bajo la expectativa de lograr un tratado internacional multilateral que, en el mejor de los casos, prohíba su desarrollo o, en su defecto, regule la materia. Las voces críticas señalan que existe una necesidad de tener pleno conocimiento sobre el uso y alcance del robot autónomo. Saber dónde y cuándo se utiliza la fuerza y que esa decisión dependa de un ser humano. Se asocia también el riesgo de utilización por parte de Estados totalitarios o agrupaciones terroristas, haciendo más eficaz la cibercriminalidad. El mayor riesgo lo supone la circunstancia fáctica de una dificultosa trazabilidad de la decisión del sistema autónomo, siendo incierta la posibilidad de atribuibilidad del acto y deconstrucción del proceso decisional del autómata, encontrándose nuevamente ante un algoritmo de caja negra.

Por otra parte, en medio de esta discusión, la Comisión de Asuntos Jurídicos del Parlamento Europeo aprobó un documento regulatorio en la consideración de que nos encontramos en la cuarta Revolución Industrial y la que podría ser la revolución de las revoluciones.

Se consideró importante destacar como directrices la protección del ser humano ante la incorporación de robots a la vida cotidiana, la oportunidad de rechazo de la atención terapéutica por parte de estos, la necesidad de proteger la libertad y privacidad humana frente a estos ante distintas injerencias fundadas en pretextos de protección o tutela, el recelo en el manejo de datos personales, el cuidado ante la manipulación ante la empatía artificial, el cuidado ante la distorsión de los

vínculos sociales por interferencia o aislamiento, y la necesidad de un amplio debate ético sobre el acceso humano a tecnologías de mejora.

Las tensiones entre la innovación y el riesgo de perder el control sobre la tecnología, marcan la firme preocupación por la trazabilidad de los sistemas autónomos y la necesidad de orientar todo desarrollo basándose en principios de beneficiencia, no maleficiencia, autonomía y justicia, dignidad humana, igualdad, equidad, no discriminación, consentimiento informado, privacidad y protección de datos.

En este marco se debatió la cuestión de la conciencia en la inteligencia artificial y se concluyó que las leyes sobre robótica de Asimov deben considerarse dirigidas a diseñadores, productores y operadores de IA, en la medida en que dichas leyes no podrían convertirse en codificaciones programables.

En las definiciones del Parlamento Europeo, se caracterizó dentro de una de las subcategorías de la IA a los sistemas autónomos capaces de adquirir independencia mediante el intercambio de datos con el entorno (interconectividad) y el análisis de dichos datos. También por la capacidad de aprender a través de la experiencia y la interacción, por un lado y, por el otro, por la extensión física de la influencia del sistema o su soporte físico. Por último, y más relevante, por la capacidad de adaptar el comportamiento y acciones al entorno.

En este punto, la definición de autonomía es clave. En la resolución citada, en el tramo relativo a "responsabilidad", se precisó que la autonomía de la IA es la capacidad de tomar decisiones y aplicarlas al mundo exterior, con independencia de todo control o influencia externos, siendo esta de carácter tecnológico.

Enfoque

La criminalidad se manifiesta en aquellos espacios donde las regulaciones que tienden a proteger la confiabilidad de las relaciones interpersonales, hoy día intermediadas por los abrigos de la tecnología digital, llegan de modo tardío o ineficaz. Muchas veces las normas son anacrónicas y otras tantas sobreprotectoras y restrictivas hacia el impulso de la innovación y desarrollo, generando la aparición de mercados negros.

El escenario contextual de la era digital ha venido a presentar numerosos desafíos al efecto de las diversas temáticas que hoy nos ocupan en este dosier a iniciativa del Consejo de la Magistratura de la Ciudad de Buenos Aires, donde tanto los delitos en particular ya legislados en nuestro medio, como las nuevas prácticas o conductas surgidas al amparo de las nuevas tecnologías, hábitos y costumbres de la cultura digital, permiten además que se incluya en la discusión el papel de los nuevos sistemas autónomos bajo estructuras de aprendizaje profundo y su injerencia en diversas formas de criminalidad.

A su vez, este aspecto o componente novedoso del problema, nos lleva a reflexionar sobre diversas posibilidades no lejanas que estarán presentes en nuestra realidad y sobre las que habrá que repensar los esquemas normativos para discernir responsabilidades jurídico-penales derivadas del activo protagonismo de estas tecnologías, tanto a través de la *web*, como de los sistemas de red cerrados pero con injerencia en la individualidad de los sujetos vinculados a las actividades sociales a los que esos sistemas estén destinados.

De esta manera podemos identificar distintos escenarios donde la inteligencia artificial, bajo tecnologías de aprendizaje profundo, pueda tener protagonismo a la hora de cometerse un crimen.

Propiamente, los sistemas que operen en la *web* son el escenario primero para estudiar. En segundo término, los ámbitos públicos o privados en donde existan redes de uso restringido, que tengan injerencia sobre la administración de entidades públicas, privadas, tales como empresas, asociaciones civiles, e incluso aquellos sistemas informáticos que tengan virtualidad de conectarse con la intimidad de un domicilio, ya sea las llamadas casas inteligentes o si se quiere simples sistemas de vigilancia remota vinculados a dispositivos de control a través de la *web*.

En tercer lugar, aquellos sistemas autónomos que se sirvan de soportes físicos para ejecutar sus funciones. Aquí podemos incluir muchos ejemplos que he venido tratando como los sistemas de navegación en transportes autónomos y la mayoría de los desarrollos en robótica.

El problema de estos escenarios es que nos encontramos a las puertas de la disolución de los límites digitales a espacios meramente computacionales. Si hoy día parte de nuestra amplia universalidad que nos personaliza se encuentra anclada en sistemas informáticos de bases de datos estatales como los de previsión social e impositiva, así como en

entidades privadas, ya sean redes sociales, registros comerciales, bancarios o incluso del sistema de salud público o privado, nos encontramos a pasos de que la interacción de datos fluya de un modo más dinámico y difícil de percibir o identificar en espacios "físicos" o su contrario.

La sociedad avanza hacia una estructura digital que, en palabras del Parlamento Europeo, exige una conectividad ubicua, aspirando a una integración plena de la red bajo el principio de neutralidad, aceptando que la interoperatividad entre los sistemas, dispositivos, registros de datos, servicios de nube, es indispensable para que el flujo promueva un entorno dinámico transparente y de acceso igualitario.

De esta forma, los espacios tradicionales del cibercrimen a través de la *web* no se reducen a este ámbito y se ven ampliados a los escenarios en donde la tecnología avanza. Hoy día se realizan intervenciones quirúrgicas remotas a través de sistemas con soporte físico. Desde el sistema de cirugía robótica Da Vinci de la firma Intuitive Surgical, pasando por el sistema PRECEYES del Área de Neurociencia Clínica del Departamento Nuffield de la Universidad de Oxford, hasta los buques mercantes no tripulados aprobados por la clasificadora naval Lloyd's Register de Londres, los sistemas de vigilancia por reconocimiento y sistemas autónomos robóticos para la atención terapéutica, educativa, y aquellos diseñados con fines bélicos, tenemos una gama variada y creciente a la cual deberá añadírsele la utilización de las nuevas tecnologías, particularmente aquellas que los doten de mayor autonomía e independencia, acercándose rápidamente a la consciencia digital.

Sobre este último punto es que habré de focalizar mi aporte, analizando las variantes de la criminalidad digital en tiempos de avances notorios de los sistemas autónomos en la vida cotidiana, y particularmente me inclinaré por abordarlo desde la difícil temática de la autoría y participación.

Personalidad jurídica y capacidad de conducta. Personalidad jurídica electrónica o digital

La dogmática penal:

> Hace posible [...] al señalar límites y definir conceptos, una aplicación segura y calculable del Derecho penal, hace posible sustraerle de la

> irracionalidad, de la arbitrariedad y de la improvisación. Cuanto menos desarrollada esté la dogmática, más imprevisible será la decisión de los tribunales, más dependerá del azar y de factores incontrolables la condena o la absolución. Si no se conocen los límites de un tipo penal, si no se ha establecido dogmáticamente su alcance, la punición o impunidad de una conducta no será la actividad ordenada y meticulosa que debería ser, sino una cuestión de lotería. Y cuanto menor sea el desarrollo dogmático, más lotería, hasta llegar a la más caótica y anárquica aplicación de un Derecho penal del que –por no haber sido objeto de un estudio sistemático y científico– se desconoce su alcance y su límite.[4]

Es precisamente un tema dirimente en dogmática penal, aquel que se ocupa de la intervención en el delito, concretamente de la autoría y participación.

Naturalmente no existe acuerdo sobre muchos aspectos en este tema, pero como ha señalado Yesid Reyes Alvarado muchos de los problemas de las discusiones dadas en ciencia penal no naufragan por falta de fundamentos, sino por falta de acuerdo sobre las bases sobre las cuales se discute.[5] Aquí son claves los conceptos de acción y de allí el alcance de otros institutos como el de imputación objetiva.

> Pese a que la intervención de una pluralidad de personas en una obra es un acontecer propio de la vida corriente, se mantiene una larga disputa entre quienes sostienen que los conceptos de autor y de partícipe son elaboraciones puramente legislativas, y quienes postulan que la ley debe respetar los datos de la realidad que le vienen dados por la existencia cotidiana [...] De admitirse la primera tesis, el legislador podría negar cualquier diferencia entre autor y partícipe, plegándose a la llamada tesis del autor único, para la cual es autor todo el que hace cualquier aporte al delito, sea como autor o partícipe [...] Desde la perspectiva contraria [...] no se pone en duda que la ley puede desvalorar las conductas de distinta forma, pero lo que no puede alterar es el objeto de la valoración, pues se trata de una ligadura funcional a la realidad que la teoría penal no puede desconocer en ningún ámbito y, por supuesto, tampoco en el de la participación. Es incuestionable que desde el idealismo siempre se

4. Ambos, Kai, "Dogmática jurídico-penal y concepto universal de hecho punible" *Política Criminal*, Vol. 3, Nº 5, 2008, A6-5, pp. 1-26, con cita de Gimbernat, Enrique, "Hat die Strafrechtsdogmatik eine Zukunft?", ZStW. 82 (1970), p. 405 y ss.

5. Reyes Alvarado, Yesid, "El concepto de imputación objetiva", en *El Derecho Penal Contemporáneo*, Nº 1, Ed. Legis, p. 5.

> pretenderá que estos conceptos son de factura legal, lo que será rebatido desde un punto de vista realista: si, comenzando por la conducta, se niega al legislador la posibilidad de alterar los datos de realidad al construir cualquier concepto jurídico-penal, es una necesaria consecuencia que tampoco puede alterar la sustancia del concepto de autor o partícipe en la misma. En este caso –al igual que en el de la acción– esto no obedece a que lo óntico determine la función de los conceptos penales, y menos aun los conceptos mismos, sino a que las categorías jurídico-penales, si bien tienen siempre una función política, debe ser construidas a su medida, pero con los límites que establece la realidad, pues de lo contrario no se realizaría más que el ocultamiento de su verdadera función política.[6]

Por su parte, ha sido Roxin quien sostuvo que

> El concepto unitario de autor persigue la finalidad de hacer mayormente superflua la a menudo difícil delimitación de la autoría, inducción y complicidad y así simplificar la aplicación del Derecho. No obstante, debe preferirse [...] la tripartición de la formas de intervención. Esta satisface la exigencia propia de un Estado de Derecho de que la punibilidad ha de fundarse en la realización del tipo y referirse a ella.

A esto agrega con énfasis "la teoría unitaria de la autoría da lugar a una intolerable ampliación de la punibilidad por la reducción de la realización típica a la causalidad".[7]

Tenemos entonces dos puntos de vista que a pesar de partir de concepciones disímiles, concurren en encontrar una necesidad de anclar los conceptos en esquemas que se refieran a las conductas que prescriben las normas y que no deriven en una ampliación intolerable del horizonte prohibitivo.

Dirá Zaffaroni que nuestro sistema constitucional y legal, se inclina por el respeto a los elementos de la realidad y que el Código Penal refleja esa decisión constitucional.

El problema con esta afirmación es que se enfrenta a un renacido rival con la sanción de la Ley N° 27401, en la medida en que ha puesto en tela de juicio el criterio de doble jurisdicción de la Corte Suprema en materia de casos en donde se encuentra vinculada una

6. Zaffaroni, Eugenio R.; Alagia, Alejandro y Slokar, Alejandro, *Manual de Derecho Penal. Parte General*, Ed. Ediar, 2da edición, 2002, p. 768.

7. Roxin, Claus, *Derecho Penal. Parte General*, Buenos Aires, Ed. Thomson Reuters-Civitas, 2014, T. II, p. 65.

persona jurídica y de allí la necesidad de explicar y refundar la posibilidad de sometimiento a proceso, capacidad de conducta, naturaleza de la pena, etcétera. Por cierto, no es el objetivo de este artículo ingresar en un tema tan imbricado como el de la posibilidad de que las personas jurídicas sean responsables penalmente, pero lo claro aquí es que la ley ha significado una clara postura del legislador en favor de la imputación de estos entes. En el decir de Castex y Dubinski: "Hay verdades que el tiempo desvanece o la política criminal globalizada derrota. *Societas delinquere non potest* es una de ellas".[8]

La afirmación en contrario sólo puede prosperar al normativizar el concepto de conducta. Es claro que las teorías del causalismo y finalismo construyeron sus esquemas a partir de nociones tales como la causalidad e intencionalidad, propias de las ciencias naturales. Es por ello que se elaboraron aspectos objetivos y subjetivos, como representaciones de lo que sucede en el mundo de las cosas y en el de las ideas, dentro y fuera de la mente del individuo. Se trata de concepciones ontológicas de la teoría del delito.

Por contrapartida, una concepción normativa de la teoría del delito,

> … comienza por admitir que el hecho punible no es un fenómeno natural, sino producto de la vida del ser humano en sociedad […] lo que se intenta poner de relieve es que el eventual reproche que esas conductas merezcan no resulta de su apreciación como meras manifestaciones ontológicas del intelecto humano, sino de la comparación del comportamiento efectivamente realizado con aquel que socialmente se esperaba del autor.[9]

Se afirmará entonces que la base de una responsabilidad penal radica en los ámbitos de competencia de cada individuo, pues sólo a quien respecto de determinadas actuaciones posee una posición de garante puede serle reprochado su comportamiento desviado. Esa responsabilidad es ponderada también en orden a la concepción normativa de la adecuación social. Esto es, que

> … no toda lesión ni puesta en peligro de los bienes jurídicos le interesa al derecho penal y, por consiguiente, ni la vulneración causal de un inte-

8. Castex, Francisco (dir.); Dubinski, Andrés M. y Martínez, Sebastián (coords.), *Responsabilidad Penal de la Persona Jurídica y Compliance*, Buenos Aires, Ed. Ad-Hoc, 2018, p. 35.

9. Reyes Alvarado, Yesid, *op. cit.*, pp. 27 y 28.

> rés jurídico (como parecía desprenderse de una concepción causalista), ni su intencional agresión (conforme a los planteamientos de corte finalista) son elementos que permiten distinguir aquellas conductas que le incumben al derecho penal de las que deben permanecer al margen de su atención. Lo que en verdad interesa al derecho penal es la forma de ataque al bien jurídico...".[10]

En ese marco, para esta postura

> Así como la teoría del delito no debe ser edificada tomando como eje central de la misma conceptos extraídos de las ciencias naturales, así mismo la distinción entre lo que debe formar parte de los aspectos objetivo y subjetivo del delito debe ser elaborada con parámetros diversos de los meramente ontológicos. De esta manera, en una concepción normativa de la teoría del delito [...] la diferencia entre las esferas objetiva y subjetiva no depende de que los elementos que las componen se hallen dentro o fuera de la mente del ser humano, como sí ocurría en las concepciones causalista y finalista. Por el contrario, mientras lo objetivo será el estudio de la conducta del hombre en cuanto ser social, lo subjetivo hará referencia al análisis del comportamiento del hombre en cuanto individuo; desde el punto de vista nominal, el primero de dichos aspectos recibirá el nombre de imputación objetiva, al paso que el segundo será denominado imputación subjetiva.[11]

Ninguna duda cabe a esta altura que el concepto de acción es un concepto jurídico. Zaffaroni sostiene que el propio Welzel lo entendió así, pero insistía en que el concepto jurídico no podía inventar lo que en el mundo no existe.

> Es [...] inevitable que [...] la acción sea, para el derecho penal, un concepto jurídico y no un mero dato de la realidad. No se trata de una decisión del penalista sino de una condición que no puede eludir: es una condición óntica.[12]

Sin embargo, "No hay [...] un concepto óntico de acción, pero hay límites a la construcción jurídico penal del concepto de acción".[13]

La base legal de construcción del concepto de acción según este autor, radica en la Constitución misma:

10. Ibídem, p. 30.
11. Ibídem, p. 31.
12. Zaffaroni, Eugenio R.; Alagia, Alejandro y Slokar, Alejandro, *op. cit.*, p. 414.
13. Ibídem, p. 415.

> El hecho del proceso y de la causa (art. 18) sería una base bastante sólo y, más aun, las acciones del art. 19, que a contrario sensu serían acciones públicas (o privadas con implicancia pública) las únicas que admiten la intervención estatal. Para mayor claridad, conforme a la incorporación del art. 75 inc. 22 constitucional, se exige expresamente en varios textos de derecho internacional de los derechos humanos que sólo puedan configurar delitos las acciones u omisiones (art. 11, 2° párrafo de la DUDH; art. 15 párrafo 1° del PIDCP; art. 9° de la DADH; art. 40, párrafo 2° apartado "a" de la Convención sobre los Derechos del Niño).[14]

Habrá entonces una inevitable tensión de la nueva ley con la hermenéutica de la arquitectura constitucional de las posturas finalistas que anclan los conceptos jurídicos en elementos ontológicos. Necesariamente habrá que conciliar para estos autores la ley a una teoría de doble jurisdicción, quedando fuera aspectos de punición –por inconstitucionalidad– en lo que se refiere al hecho punible en forma autónoma por la persona jurídica.

Para las posturas funcionalistas o normativistas, no habrá ningún obstáculo en la construcción de conceptos que permitan imputar a estos entes de manera equidistante con la persona humana.

Esta disquisición tendrá mayor valor al retomar el encuadre jurídico de los actos de los sistemas autónomos bajo tecnologías de aprendizaje profundo y toma de decisiones escalonadas o por redes neuronales.

Sorteando esta discusión y admitiendo la hipótesis de que es posible la imputación a las personas jurídicas, me interesa ahora señalar que la ley prevé una taxonomía cerrada sobre la cual es posible la imputación a una empresa. No obstante estos escasos delitos aplicables, la postura legislativa admite la responsabilidad del ente cuando se hubieren realizado directa o indirectamente "con su intervención", "en su nombre", "interés" o "beneficio", y así también cuando aquel que hubiere actuado en "beneficio o interés de la persona jurídica fuere un tercero que careciese de atribuciones para obrar en representación de ella, siempre que la persona jurídica hubiese ratificado la gestión, aunque fuere de manera tácita".

Según Yacobucci, el contenido material de la responsabilidad de la persona jurídica reside principalmente en los defectos de la configuración de su cultura ética. Esta falla de configuración se identificó en

14. Ídem.

la ausencia de sistemas de controles y supervisión como trazo integral de la persona jurídica.[15]

Sostiene el jurista que

> ... la justificación de la responsabilidad del ente se funda en una configuración "interna" de la corporación que la ubica en contradicción o infidelidad para sus deberes con el orden jurídico. Esa criminalidad corporativa, que se expresa en la noción de Unrechtssysteme –Lampe–, implica identificar una actitud organizativa defectuosa, aunque pueda exteriorizarse a través de distintos niveles o intensidades (LAMPE, Ernst-Joachim, "La dogmática jurídica penal entre la ontología social y el funcionalismo", Ed. Grijley, 2003).[16]

La Ley N° 27401 establece en los artículos 22 y 23 la posibilidad de implementar programas de integridad, que no son otra cosa que el contenido propio de lo que se conoce como "*compliance*".[17]

15. Yacobucci, Guillermo J., "La empresa como sujeto de imputación penal", en *La Ley*, año LXXXI, N° 225, 2017.

16. Ídem.

17. Ley N° 27401: "Art. 22. Programa de Integridad. Las personas jurídicas comprendidas en el presente régimen podrán implementar programas de integridad consistentes en el conjunto de acciones, mecanismos y procedimientos internos de promoción de la integridad, supervisión y control, orientados a prevenir, detectar y corregir irregularidades y actos ilícitos comprendidos por esta ley.
El Programa de Integridad exigido deberá guardar relación con los riesgos propios de la actividad que la persona jurídica realiza, su dimensión y capacidad económica, de conformidad a lo que establezca la reglamentación".
"Art. 23. Contenido del Programa de Integridad. El Programa de Integridad deberá contener, conforme a las pautas establecidas en el segundo párrafo del artículo precedente, al menos los siguientes elementos:
a) un código de ética o de conducta, o la existencia de políticas y procedimientos de integridad aplicables a todos los directores, administradores y empleados, independientemente del cargo o función ejercidos, que guíen la planificación y ejecución de sus tareas o labores de forma tal de prevenir la comisión de los delitos contemplados en esta ley;
b) reglas y procedimientos específicos para prevenir ilícitos en el ámbito de concursos y procesos licitatorios, en la ejecución de contratos administrativos o en cualquier otra interacción con el sector público;
c) la realización de capacitaciones periódicas sobre el Programa de Integridad a directores, administradores y empleados.
Asimismo, también podrá contener los siguientes elementos:
I. el análisis periódico de riesgos y la consecuente adaptación del programa de integridad;
II. el apoyo visible e inequívoco al programa de integridad por parte de la alta dirección y gerencia;

Se trata de un sistema que

> … tiene por objeto establecer mecanismos de prevención de conductas delictivas dentro de las empresas y delimitar la responsabilidad penal individual de las personas involucradas en ella, ya que la estructura de relaciones de una compañía conforma un ámbito propicio para diluir la responsabilidad de los intervinientes.[18]

De esta forma, el fundamento que define el sustrato sobre el cual se infiere el hecho comportamental del ente jurídico tiene que ver con una serie de condiciones que hacen a un programa de contención de riesgos asociados a la actividad o tráfico económico que suponen los emprendimientos colectivos asociados en categorías societarias formales.

No cabe duda aquí que el contenido de injusto se nutre de autoformulaciones del sistema normativo que enuncia y define sus conceptos desde el propio ámbito normativo, sin representatividad ontológica.

Klaus Volk estudió el problema de tratar de representar la realidad a través de un lenguaje analítico que en ciencia jurídico penal se manifiesta a través de la dogmática. Escribió que "La empresa rigurosamente empirista de remitir todo a lo 'observable' ha fracasado desde hace mucho".[19]

III. los canales internos de denuncia de irregularidades, abiertos a terceros y adecuadamente difundidos;
IV. una política de protección de denunciantes contra represalias;
V. un sistema de investigación interna que respete los derechos de los investigados e imponga sanciones efectivas a las violaciones del código de ética o conducta;
IV. procedimientos que comprueben la integridad y trayectoria de terceros o socios de negocios, incluyendo proveedores, distribuidores, prestadores de servicios, agentes e intermediarios, al momento de contratar sus servicios durante la relación comercial;
VII. la debida diligencia durante los procesos de transformación societaria y adquisiciones, para la verificación de irregularidades, de hechos ilícitos o de la existencia de vulnerabilidades en las personas jurídicas involucradas;
VIII. el monitoreo y evaluación continua de la efectividad del programa de integridad;
IX. un responsable interno a cargo del desarrollo, coordinación y supervisión del Programa de Integridad;
X. el cumplimiento de las exigencias reglamentarias que sobre estos programas dicten las respectivas autoridades del poder de policía nacional, provincial, municipal o comunal que rija la actividad de la persona jurídica".

18. Castex, Francisco (dir.); Dubinski, Andrés M. y Martínez, Sebastián (coords.), *op. cit.*, pp. 40 y 41.

19. Volk, Klaus, *La verdad sobre la verdad y otros estudios*, Buenos Aires, Ed. Ad-Hoc, 2007, p. 45.

Remarcó que existen "disposiciones" que no se estiman detectables de forma directa, sino que se requiere y se hace imprescindible, ubicar el comportamiento en determinadas situaciones. El predicado disposicional "acepta la posibilidad de captar un 'significado contextual y estructural remanente', tal como puede observarse ante un trasfondo social, cultural e histórico (que los empiristas duros probablemente rechazarían siempre como 'metafísica')". Y agrega

> La solución más plausible consiste en introducir conceptos disposicionales como teoréticos. La teoría llama a este fundamento "de los dos niveles". En efecto, establece dos niveles de lenguaje: uno observacional, y otro teórico con el que ella se formula a sí misma.[20]

Al referirse a la relación derecho-prueba explica que, por ejemplo, el concepto jurídico penal de dolo puede ser justificado desde el saber psicológico o simplemente supuesto como una ficción necesaria desde el ámbito jurídico. En definitiva, subraya que

> Los conceptos teoréticos siempre se completan parcialmente con contenido empírico. Por lo tanto, carece de sentido exigir de antemano "pruebas empíricas" completas y, como se ha mostrado, tampoco se debe exigir que cada concepto teorético deba vincularse inmediatamente con la "realidad" mediante reglas de coordinación.

Lo que sucede con la prueba de un concepto, sucede al nivel de la acreditación teorética. Aquellos elementos observables tamizados por la consideración teorética (esto es: significado contextual en orden a un trasfondo social, cultural e histórico), concluyen en el contenido de una proposición afirmativa sobre la existencia de una situación (justificación).[21]

En la teoría del doble nivel entonces, funcionan proposiciones que definen el contenido fáctico y proposiciones que definen relaciones sistemáticas y dogmáticas desde la perspectiva pragmática.[22]

En definitiva, sostiene el autor, "La discusión sobre una teoría normativa o descriptiva es una discusión sobre la ciencia y su praxis;

20. Ibídem, p. 46.
21. Ibídem, p. 53.
22. Ibídem, p. 56.

en consecuencia, una discusión sobre la 'praxis social' y con ello una discusión sobre posiciones políticas".[23]

Parte de esta elaboración de conceptos jurídicos tiene vinculación con una relación que haré de seguido que parecerá un tanto asintomática, pero tendrá su función en la línea argumental que propongo.

En 2014, la Corte Suprema de Justicia de la Nación rechazó por cuestiones formales un hábeas corpus interpuesto en favor de un chimpancé llamado Toti. Fue una primera aproximación a lo que luego ocurriría con la orangutana de Sumatra llamada Sandra, cuando la Sala II de la Cámara Federal de Casación Penal, sobre la base de una interpretación jurídica dinámica y no estática, consideró menester reconocerle el carácter de sujeto de derechos, en la medida en que –afirmaron– los sujetos no humanos –animales–, son titulares de derechos por lo que corresponde su protección.[24]

Por su parte, la justicia de la Ciudad hizo lugar al amparo que demandaba la protección de Sandra, considerando que esta era víctima de lo que se denomina especismo antropocéntrico, destacando que los orangutanes son seres pensantes, sintientes, inteligentes y genéticamente similares a los seres humanos, con similares pensamientos, emociones, sensibles y auto reflexivos; que tienen cultura, capacidad de comunicarse y un rudimentario sentido del bien y del mal; una individualidad propia, con una historia, carácter y preferencias únicas.

En este marco, verá el lector que la plasticidad de nuestro sistema normativo admite asignarle rasgos comportamentales a entes jurídicos incapaces de acción en sentido biológico, no obstante lo cual resultan pasibles de responsabilidad penal, y asimismo se admite la asignación de la calidad de sujeto de derechos a seres que no obstante no ser personas ni humanos, reciben protección jurídica por el expreso reconocimiento derivado de tratarse de sujetos no humanos titulares de derechos.

Bajo este lineamiento, han sido numerosas las opiniones en lo que hace a la naturaleza jurídica que correspondería asignarle a los sistemas autónomos que se acerquen a niveles de consciencia elevados y cuyo rol en la realidad social podría llevarlos a un protagonismo cotidiano

23. Ibídem, p. 60.

24. CFCP, "Orangutana Sandra s/ recurso de casación s/ hábeas corpus", Sala II, causa N° 68831/2014/CFC1, rta. del 18/12/2014.

que demande características especiales de regulación que clarifiquen lo que se espera del sistema autónomo, del diseñador, del productor, del comerciante, del usuario y del Estado como garante último.

El debate dado en este punto se dirime entre la existencia o no de una necesidad práctica de identificar las responsabilidades por los diseños, desarrollos, productos y usos de la inteligencia artificial. Se postula por un lado la posibilidad de brindarle la calidad de persona jurídica digital a aquellos sistemas autónomos que tengan un desarrollo de elevado nivel de toma de decisiones o "consciencia", en función de las nuevas tecnologías de aprendizaje profundo por redes, capas o encadenamientos neuronales.

La sustancia de la discusión se circunscribe a los sistemas autónomos de uso bélico, industrial y doméstico, lo que compone básicamente los tres perfiles del impacto de la inteligencia artificial en los desarrollos actuales. Ya sea que se trate de personas jurídicas digitales, electrónicas, sujetos de derecho no humanos o de entes capaces no personales con individualidad digital, lo determinante es el producto de la nominación jurídica que las categorías legales impregnen en esta realidad tecnológica naciente. La dialéctica entre el anacrónico lenguaje jurídico y la propia tecnología derivará en las lógicas sobre la base de las cuales se establezca y consolide la percepción y consecuente aceptación de la IA en la era digital.

De tal manera que las regulaciones sobre las responsabilidades de estos entes podrían recibir legislación que opere a nivel administrativo y en función de una doble jurisdicción establecer respuestas acordes a la nueva realidad. Asimismo y en nuestro medio, la plasticidad de la legislación actual ya señalada podría incluso permear el debate sobre la máxima *societas delinquere non potest*, herido por la Ley N° 27401, y asignar con criterio utilitario o pragmático personalidad jurídica o la nominación de la que se trate.

Piénsese en el caso de un sistema autónomo, cuyos algoritmos de aprendizaje lo llevasen a tomar decisiones que afecten la libertad o vida de un ser humano. Se observa de lo expuesto en este artículo un primer problema dado por la trazabilidad del proceso decisional del sistema y con este la responsabilidad del diseñador, del productor, del comerciante y así también del usuario.

Piénsese en sistemas que podrían lanzarse al mercado con códigos fuente cerrados, pero así también abiertos, donde la complementación de la programación llevada adelante por el usuario podría derivar en responsabilidad de este y no del diseñador. Piénsese en la posibilidad de reprogramar sistemas autónomos comercializados lícitamente en el mercado con fines espurios, trasladables a organizaciones criminales o terroristas.

Basta aquí presentar esta problemática y traer un ejemplo claro sin zonas de penumbra. El Ministerio de Transportes e Infraestructuras Digitales de Alemania conformó un comité de expertos para elaborar un Código de ética para el funcionamiento de los vehículos autónomos y así dar respuestas a interrogantes tales como los que presenta el dilema del tranvía.

¿Debería el sistema autónomo atropellar a cinco personas atadas en la vía, o debería accionar el mecanismo para desviarse y atropellar y matar a otra persona que se encuentra atada en la vía auxiliar?

Según los expertos germanos, el vehículo autónomo no debe "interpretar" las leyes, sino aplicar las normas de tráfico a rajatabla y minimizar los daños en la medida de lo posible. Si el atropello es inevitable, el sistema no debe jamás "establecer preferencias en base a la edad, sexo o condiciones físicas o mentales de los afectados".

En el dilema del tranvía, según los expertos, el sistema debería mantener el rumbo e intentar evitar la colisión pero no debería dotarse a la IA de la posibilidad de seleccionar entre una vida u otra.

Más allá de estos problemas que ya son actuales, me interesa hacer foco sobre horizontes no tan lejanos, en las cuales los sistemas autónomos más avanzados se presentarán con complejos entramados de procesamiento en donde la posibilidad de conocer y trazar la etiología de la decisión del sistema será casi tan compleja como inaccesible.

Y aquí aparece un concepto más caótico, llamado "singularidad tecnológica", respecto del cual considero que representa el paradigma de la era digital y es el que deberá estructurar el pensamiento humano frente a los desarrollos a futuro. Se trata del momento en el cual la IA se encontrará en condiciones de crear sus propios sistemas, que por capacidad de procesamiento, perfeccionamiento y efecto iterativo, importará una superación inconmensurable en el desarrollo de la ciencia y la técnica.

Nos encontramos más cercanos en el tiempo a la posibilidad de que ocurra con la aparición de la tecnología *deep learning*. En este sentido, los problemas de trazabilidad e independencia de ciertos sistemas ante la evolución de su complejidad y capacidad de respuesta, son los que interesarán en el enfoque aquí propuesto para analizar responsabilidades producto del tráfico de estas tecnologías en nuestra actualidad.

Notas pertinentes de autoría y participación

Estonia es noticia por autoproclamarse como nación digital. Casi la totalidad de los trámites estatales son canalizados vía digital. Los ciudadanos poseen una carta civil digital, con la cual acceden e interactúan en los diversos estamentos de la sociedad civil. Tanto en el sistema estatal público como en entidades privadas, comerciales o sanitarias, los ciudadanos digitales se conducen a través de Internet y sólo respecto de escasos trámites se demanda su presencia física.

A pesar de la distancia con esta realidad, en nuestro país existen numerosas bases de datos, crecientes, en las cuales se depositan registros de datos personales, privados, en función de los cuales poseemos la posibilidad de interactuar en la sociedad civil. Piénsese en lo más rudimentario y sencillo, como un alta laboral bajo una clave de identificación, un registro activo de contribuyente, el alta en un empleo público o privado, una historia clínica digital, un usuario de *home-banking*, el correo electrónico, los discos virtuales, las nubes, hasta la propia identidad digital transcurrida en la interacción social que proponen las nuevas tecnologías, todo tiene su correlato en bases de información, en discos o nodos duros de almacenamiento.

En estos casos, la cibercriminalidad más habitual es la que se produce cuando estas bases de datos, cualesquiera que se elija, son vulneradas o accedidas. Hoy día y con la aparición del *blockchain*, resulta prácticamente imposible vulnerar sistemas complejos. Podrán atacarse determinadas terminales físicas, pero dado que la información es compartida y producida a escala, resulta prácticamente imposible provocar un ciberataque de esa magnitud. Actualmente, el *bitcoin* primero y la mayoría de las criptomonedas creadas a su semejanza después, se

basan en la tecnología de "cadena de bloques" –*blockchain*–, considerada la máquina de vapor de la era digital.

Bajo este escenario resulta difícil conocer y determinar las responsabilidades derivadas de los accesos prohibidos como los que la ley argentina regula en los artículos 153 *bis* o 157 *bis* del Código Penal, por citar algunos ejemplos.

A la dificultad de investigación de esta temática se le suman la aparición de sistemas autónomos que, bajo esquemas de algoritmos de aprendizaje profundo, pueden intermediar entre el sujeto activo de la conducta y el resultado contemplado en la norma, y así también llegar a la indeterminación del sujeto humano detrás de la codificación algorítima por un simple problema de trazabilidad. Quién lo programó, dónde, cuándo, qué instrucciones recibió el sistema autónomo, por qué accionó de la forma en la que lo hizo, qué registros accedió y qué hizo con la información obtenida.

A modo de ejemplo, piénsese en todas las imágenes captadas por drones, por vehículos autónomos de transporte de pasajeros o mercaderías, la información compilada por servicios de correo, buscadores, redes sociales. Véase la permeabilidad de los datos y la falibilidad de su reaseguro bajo condiciones extremadamente frágiles.

Ante estos aspectos de difícil abordaje, el derecho penal mantiene estructuras de atribución de hechos al señorío de los sujetos que ofrecen dificultad mayúscula para tamizarlos, como veremos brevemente de seguido.

En efecto, para la teoría objetivo formal autor es quien realiza la acción típica o alguno de sus elementos. En palabras de Cerezo Mir:

> El problema con que tropieza esta teoría es que no permite comprender los supuestos de autoría mediata. La autoría mediata consiste en que una persona utiliza a otra como instrumento para cometer el delito. En estos casos el sujeto que está detrás del instrumento no realiza generalmente elemento alguno del tipo y podría ser considerado autor según esta teoría.[25]

Beling es el responsable de la distinción entre tipicidad estricta y amplia para definir al coautor y al cómplice. Fue Gimbernat Ordeig quien señaló que para Beling "Coautoría es conjunta 'ejecución' = realización de acciones que pertenecen al núcleo del tipo [...] Complicidad

25. Cerezo Mir, José, *Derecho Penal. Parte General*, Buenos Aires, Ed. BdeF, 2008, p. 929.

es realización de una acción preparatoria o de una acción accesoria para la acción ejecutiva de otro sujeto".[26] El problema de la teoría objetivo formal es que no tiene forma de explicar la autoría mediata.

Por su parte, en la teoría subjetiva

> Se parte de la teoría causal de la condición y, en base a ella, se niega toda distinción objetiva entre la actividad del autor y la del cómplice: ambos no hacen más que colocar una condición del resultado, y una condición no es posible distinguirla de otra condición. El razonamiento a que entonces se acude es este: la ley positiva distingue entre autor y cómplice; las actividades del autor y cómplice no se distinguen objetivamente; luego la distinción –impuesta por la ley– debe hallarse en el terreno subjetivo.[27]

Para Roxin,

> Según [...] [la] teoría [subjetiva] del dolo, el autor posee una voluntad independiente y el partícipe una voluntad dependiente [...] De un modo diferente, la teoría del interés parte de la base de que la voluntad del autor se caracterizaría por el interés propio en el hecho y la del partícipe por la falta de tal interés.[28]

Se dice que

> ... en el plano objetivo no pueden establecerse diferencias entre las contribuciones de los distintos intervinientes en el delito, pues todos ellos han colocado una condición para la producción del resultado. La diferencia entre las distintas aportaciones al hecho tiene que hallarse, por tanto, en el plano subjetivo. Con arreglo al concepto subjetivo, autor es el que quiere el hecho como propio, el que actúa con *animus auctoris*. En cambio, será partícipe aquel codelincuente que actúe con *animus socii*, es decir, que actúe con ánimo de ayudar, de colaborar en el hecho ajeno.[29]

Sobre esto se señaló que

> El punto de partida de esta teoría es erróneo. De la teoría de la equivalencia de las condiciones se deduce únicamente que todas las condiciones de la producción de un resultado son equivalentes desde el punto de vista causal, pero desde el punto de vista de lo injusto y de la culpabilidad

26. Gimbernat Ordeig, Enrique, *Autor y cómplice en derecho penal*, Buenos Aires, Ed. BdeF, 2006, p. 7.

27. Ibídem, p. 28.

28. Roxin, Claus, *op. cit.*, p. 72.

29. Cerezo Mir, José, *op. cit.*, p. 930.

> esas conductas pueden tener una significación muy distinta, con lo que no es cierto que no puedan establecerse diferencias desde el punto de vista objetivo entre las distintas aportaciones a un hecho. Además, esta teoría puede llevar a resultados sorprendentes, como puso de manifiesto el célebre caso de "la bañera".[30]

También con opinión crítica, Zaffaroni sostiene que "por no ser autor equivalente a causante, la extensión del concepto de autor hasta abarcar a cualquier causante es violatoria del principio de legalidad, incluso por identificar la autoría dolosa con la culposa".[31] Y agrega que "la teoría subjetiva lleva una parte de verdad, en cuanto a que no puede delimitarse la autoría sin tener en cuenta datos subjetivos, pero su fracaso obedece a que ignora cualquier dato objetivo".[32]

Por último, para la teoría final del concepto de autor, comúnmente denominada del dominio del hecho, autor es quien tiene dominio del acontecimiento.

> Se basa en la doctrina de la acción final [...] Según Welzel, autor es sólo aquel que, mediante la dirección consciente del curso causal hacia la producción del resultado típico, tiene el dominio de la realización del tipo. El autor se diferencia del mero partícipe por el dominio finalista del acontecer; el partícipe, o bien se limita a apoyar el hecho, dominado por el autor de un modo finalista, o ha determinado la resolución de realizarlo.[33]

Zaffaroni lo define como la decisión sobre la configuración central del acontecimiento "autor es quien domina el hecho, quien tiene en sus manos el curso causal, quien puede decidir sobre el sí y el cómo o –más brevemente dicho–, quien puede decidir la configuración central del acontecimiento".[34] Sostiene que

> El dominio del hecho no puede ser concebido desde una caracterización amplia del fenómeno, lo que obedece a que siempre el dominio del hecho se presenta en forma concreta, que puede ser la de dominio de la acción, de dominio funcional del hecho o de dominio de la voluntad.[35]

30. Ídem.
31. Zaffaroni, Eugenio R.; Alagia, Alejandro y Slokar, Alejandro, *op. cit.*, p. 772.
32. Ibídem, p. 773.
33. Cerezo Mir, José, *op. cit.*, p. 931.
34. Zaffaroni, Eugenio R.; Alagia, Alejandro y Slokar, Alejandro, *op. cit.*, p. 774.
35. Ídem.

La doctrina establece que la base legal para considerar que el Código Penal se funda en el criterio del dominio del hecho surge del artículo 45 del Código, cuando se refiere a los que tomasen parte en la ejecución del hecho y a los que hubiesen determinado a otros a cometerlo, e identifica al (a) autor individual (dominio de la acción), (b) autor paralelo o concomitante, (c) coautor (dominio funcional del hecho), (d) autor directo que se vale de otro que no realiza conducta, (e) autor mediato (dominio del hecho por dominio de la voluntad).[36]

Esta lectura de las normas del Código Penal de la Nación releva también la opinión de Roxin sobre la bondad de atender a una tripartición en el análisis de la intervención en el delito y también respeta por supuesto la perspectiva de un derecho penal que releve los datos de la realidad para construir las soluciones legales a los casos particulares.

Necesariamente debe existir un anclaje en la realidad, y son las normas del Código las que están estructuradas atendiendo a los principios que aconsejan anclar en la realidad todo punto de partida para la elaboración jurídica y para todo tipo de construcciones normativas que tiendan a valorar los hechos o pragmas de conflicto lesivos y relevantes en términos jurídico penales.

Ahora bien, con la distorsión de los límites ontológicos para la elaboración de conceptos penales tales como los de persona y conducta que, como bien se ha reseñado han recibido una nueva orientación del legislador en un intento por dirigir los esfuerzos normativos para controlar ciertos aspectos de criminalidad económica en el ámbito de la empresa y con ello la aceptación de la responsabilidad penal de la persona jurídica, parece tener mayor peso la opinión de Volk, quien apuntó a los problemas de utilizar esquemas tradicionales de la teoría del delito para fenómenos respecto de los cuales los conceptos que los componían no tenían la virtualidad de contemplarlos de manera efectiva, lo que denominó "la empresa observable del empirismo".

Tras la discusión sobre los límites de un derecho penal clásico o nuclear, y las formas expandidas estudiadas bajo la rúbrica de un derecho punitivo accesorio de aquel, cierto es que ante el tema central de la cibercriminalidad y la aparición de nuevas tecnologías, se observa que este fenómeno también se encuentra fuera del ámbito natural y

36. Ibídem, pp. 777 y 778.

del alcance habitual de los esquemas y conceptos tradicionales de derecho penal, de manera que para afrontarlos se hace necesario utilizar herramientas equivalentes a las que sirven de base para abordar criminalidad económica compleja.

El desafío aquí nace ante la caracterización de hechos con rasgos particulares como los que se vinculan con los sistemas autónomos y tecnologías bajo algoritmos de aprendizaje profundo y adopción de decisiones producto de entidades independientes de los diseñadores, programadores, productores, fabricantes, controladores y usuarios.

Hechos colectivos, autoría mediata, autor único o subjetivo

Sostiene Jakobs que el que comete de propia mano:

> … tiene dominio porque decide definitivamente acerca de la producción o no producción de la realización del tipo; dicho con mayor exactitud, porque sólo puede organizarse una libertad general de comportamiento si las personas al menos han de responder de las consecuencias directas, no mediadas por otros, de su conducta. Se trata, por lo tanto, del sinalagma de libertad de comportamiento y responsabilidad por las consecuencias, que constituye una configuración básica y asentada de la sociedad que abarca a todos. Por lo tanto, al principio de la imputación no está un dominio fáctico, sino una institución, y ello no sólo en los delitos de deber, sino también en el caso de los deberes […] en virtud de competencia por organización.[37]

Sobre la autoría, dice que

> No resulta posible determinar la comisión propia, la comisión de propia mano, recurriendo exclusivamente al dominio, sin la atribución de conducta y consecuencia […] Dicho de nuevo con otra formulación: ya se intuye que el dominio es una cuestión de la medida de la calificación de la intervención, una cuestión cuantitativa, mientras que la cuestión cualitativa ¿quién responde?, no se determina en función de la concurrencia

37. Jakobs, Günther, "El ocaso del dominio del hecho. Una contribución a la normativización de los conceptos jurídicos", en *Dogmática y política criminal en una teoría funcional del delito* (trad. de Manuel Cancio Meliá), Buenos Aires, Rubinzal Culzoni, 2000, p. 90.

> de dominio, sino en función de la atribución del comportamiento y de las consecuencias.[38]

En el ámbito de la codelicuencia, o multiplicidad de personas en la configuración delictiva, calificada como "dominio del coautor", Jakobs señala que

> ... solo puede llegar a haber codelicuencia si alguien ejecuta una conducta cuya continuación en una realización del tipo no ha de entenderse como puro arbitrio del sujeto que ejecuta, sino como inherente al comportamiento anterior, dicho de otro modo, su ejecución debe significar que no sólo ese comportamiento inicial, sino también el comportamiento de continuación realizado por el ulterior actuante, son asunto del autor y, en este sentido, deben serle atribuidos.[39]

En este sentido, "la codelincuencia se trata de una modalidad especial del reparto de trabajo, concretamente, de un reparto de trabajo que vincula en vez de aislar".[40]

Esta categoría será severamente criticada en doctrina por derivar en el máxima que establece que

> ... [la] ejecución no es sólo ejecución de quien ejecuta –el desnudo naturalismo de la propia mano–, sino ejecución de todos, decae la razón para destacar la ejecución por el hecho de que sólo los que ejecutan deben calificarse como autores, mientras que no deben serlo los partícipes en la fase anterior: todos los intervinientes ejecutan, con independencia de quién sea la mano que se mueva para ello.[41]

Así entonces afirma que la respuesta a la pregunta por quién tiene el dominio del hecho, es que el dominio lo posee "el colectivo".

Estas son las explicaciones de cómo se formula la idea de una intervención colectiva, un hecho colectivo que es responsabilidad de todos como autores, no sobre la base de la determinación por el criterio del dominio del hecho, sino por la delimitación valorativa del significado. Todos los intervinientes generan con su conducta una razón para que se les impute la ejecución también como ejecución suya y la razón según

38. Ibídem, p. 93.
39. Ibídem, p. 95.
40. Ídem.
41. Ibídem, p. 99.

Jakobs no se determina en función de la concurrencia de dominio, sino en función de la atribución del comportamiento y de las consecuencias.

La crítica de Schünemann se conduce a través de un claro postulado sobre la construcción de los conceptos jurídicos, dado que

> … de nuestras decisiones jurídico-constitucionales fundamentales se deriva que, en principio, la vinculación del juez a la ley, en los casos en que ella sea ontológicamente posible, también debe ser practicada, y que de ningún modo puede ser hábilmente rodeada por medio de teoremas que no son incuestionables. O, con otras palabras, mediante la metodología jurídica sólo puede dársele al juez aquellos espacios de libertad que se encuentran preestablecidos, por razones de la teoría del conocimiento y la filosofía del lenguaje, y que por eso son reconocidos por la organización del conjunto de las instituciones jurídicas que se encuentran establecidas en nuestra Constitución.[42]

Esta crítica se hace más visible cuanto el autor describe lo que entiende como el excesivo refinamiento de la dogmática penal en la sociedad posmoderna. Dice que

> … la dogmática penal se convierte (vista desde afuera) en una especie de tienda de mercaderías de toda clase, en la que la justicia encuentra en sus interminables estanterías todas las soluciones imaginables, de las que puede hacer uso, en cierto modo, a discreción.[43]

En referencia a Jakobs, Schünemann le atribuye un giro radical-normativista. Dice que este autor

> … sostuvo un regreso teórico al concepto unitario de autoría y al concepto extensivo de autor y caracterizó abiertamente a la distinción entre autoría y participación como una mera cuestión de medición de pena, a la que no corresponderían diferenciaciones concebibles cualitativamente.[44]

Esta construcción solo es posible alcanzarla en lo que en palabras de Shünemann es la adjudicación al concepto de dominio del hecho de una forma amorfa. Esto porque sostiene que el dominio del hecho se-

42. Schünemann, Bernd, *Obras*, Santa Fe, Rubinzal-Culzoni, T. I, 2009, p. 93.

43. Schünemann, Bernd, *op. cit.*, p. 491 y ss. "El dominio sobre el fundamento del resultado: Base lógico-objetiva común para todas las formas de autoría incluyendo el actuar en lugar de otro".

44. Ibídem, p. 494.

gún la perspectiva funcionalista que critica, sólo sirve para presentar la problemática pero no para deducir la solución al problema.

En su lugar se ofrece el concepto de división del trabajo vinculante. El interviniente en el hecho sería competente por la totalidad del hecho cuando hubiere proporcionado un aporte al ejecutor que lo vinculare (al interviniente) con la ejecución, por tener el sentido de darle una determinada forma a esta,

> ... el mundo exterior (y con esto se refiere Jakobs a la base ontológica del dominio del hecho) tendría una significación no como tal, sino sólo comunicado a través de la estructura normativa de la sociedad. Por eso, la distinción entre autoría y participación debería, en su opinión, ser desplazada al nivel comunicativo-simbólico del significado.[45]

Schünemann dice que Jakobs ofrece también, obviamente sin decirlo expresamente, una explicación para aquella distinción quimérica entre *animus auctoris* y *animus socii*, entre voluntad de ser autor y voluntad de ser partícipe, cuya expresión como fenómeno concebible psicológicamente fracasó por completo.

Para Jakobs lo que caracteriza a la autoría o complicidad no sería el verdadero peso causal de un aporte, sino el significado, el que sería el sentido delictivo de una aportación, por el que cada interviniente sería competente automáticamente por la totalidad del hecho.

En palabras de Schünemann, esta tesis es

> ... inaceptable [...], aunque también es muy demostrativa, pues en ella están concentrados todos los puntos débiles del normativismo radical. En primer lugar, la tesis de que el sentido delictivo de una acción convertiría al actuante en interviniente y en competente para el delito en su totalidad es desde el punto de vista lógico un mero círculo vicioso.[46]

45. Sostiene el autor aquí que "como cada interviniente será competente con respecto a la totalidad del hecho, la diferenciación entre autoría y participación recaería sólo sobre los grados de gravedad que sirven para la medición de la pena. Según esta concepción, no habría una diferenciación objetiva entre coautor y cómplice y, especialmente, tampoco una restricción de la autoría al estadío de ejecución [...] el punto central de la crítica de Roxin a la teoría subjetiva y a su aplicación por parte de una jurisprudencia centenaria consistía en que, con ella, la distinción entre autoría y participación se desplazaba completamente al nivel de la mediación de la pena". "Justamente ese desplazamiento es presentado ahora por Jakobs como la solución central del problema". Ibídem, p. 495.

46. Ibídem, p. 497.

Son los tipos penales los que describen el hecho y de este modo caracterizan al autor, como a quien pertenece esa descripción. Por eso es una noción fundamental, la que hace cuarenta años se fundó nuevamente en la acción ejecutiva descripta en el tipo penal como base de la autoría.

Con la aparición de personas jurídicas responsables en derecho penal y la flexibilización de los conceptos de un derecho penal clásico, subyacen riesgos de desdibujar el contorno de los límites de la dogmática penal y con ello una aplicación caótica.

Estas tesis naturalísticas y normativistas se encuentran en permanente tensión. La pretensión de alcanzar formas de criminalidad ajenas a toda taxonomía clásica del derecho penal, expande el alcance de las posturas normativistas y arquea los límites, en este caso, del dominio del hecho y la consecuente definición de aquello que es atribuible al sujeto en función de ser el responsable de la concreción de un resultado (ser imputable por el hecho que se le asigna a su señorío).

Estos problemas se presentan también para la determinación de las responsabilidades en materia de la realización de actos, conductas o hechos que se encuentran intermediados por programas, sistemas, aplicaciones, ejecutados a través de la *web*, sirviéndose de dispositivos o simplemente invadiendo físicamente computadoras restringidas para el autor.

La solución dogmática que nace rápidamente en estos debates es la que trata de explicar, a través de la autoría mediata, la relación de responsabilidad del autor detrás del autor mecánico o sistema autónomo que ejecuta, no ya por llevar adelante una operación para la cual ha sido programado, sino que la realiza por haber decidido mediante el procesamiento de cientos de miles de reflexiones la acción prohibida derivada del encadenamiento que integra el entramado de su pensamiento.

La acción del sistema autónomo puede ser el resultado dentro de un campo de acción previsible, pero así también puede ser producto de la independencia decisional que los algoritmos de pensamiento profundo complejos puedan dar lugar a que ocurran en los sistemas de más elevada "conciencia". Nadie podría afirmar que los programadores de Microsoft decidieron dar lugar a un *chatbot* –Tay–, que tenga manifestaciones racistas y nazis como una de las posibilidades dentro del campo de acción para el cual fue programado.

Nuevamente piénsese en los tres campos o perfiles de la IA en la realidad práctica, esto es, sistemas bélicos, industriales y domésticos. Piénsese en casos de sistemas autónomos que en el marco de acciones bélicas desatiendan los Convenios de Ginebra o el Estatuto de Roma. Que sistemas autónomos industriales o comerciales, como podría ser en el ámbito sanitario, lleven adelante acciones que lesionen la vida o salud de los pacientes. Sistemas domésticos que limiten la libertad de adultos mayores con sentido tuitivo de apariencia racional y que esas determinaciones no puedan tener una etiología atribuible al fabricante, diseñador, distribuidor, comerciante o Estado –de manera directa–, atento a la incertidumbre sobre la trazabilidad de los procesos decisionales de estos sistemas.

El problema de hacer expansiva la responsabilidad, hacia los estamentos de mayor injerencia en la puesta en funcionamiento del sistema autónomo, con títulos de coautoría bajo esquemas de dogmática normativista, supone rasgar nuevamente los límites de autoría y participación, que fueron descriptos en el debate presentado entre las posturas de Jakobs y Schünemann, sin un horizonte que nos permita clarificar el pragmatismo en la asunción de esta postura funcionalista.

En los esquemas de intervención colectiva, de encadenamiento de responsabilidades y de competencias en ámbitos de organización, la utilización de la estructura del autor mediato para explicar la responsabilidad del sujeto detrás del sujeto que ejecuta, supone el gran desencanto de poner en crisis un principio cultor de la dogmática penal: el principio de autorresponsabilidad.

Muchas veces se recurre a la coautoría con la intención de

> ... seguir otorgando responsabilidad a título de autor a quienes ordenan, desde su posición de mando dentro de la organización, la comisión de delitos, sin renunciar a la premisa, según la cual no es posible apreciar autoría mediata cuando el ejecutor material responde penalmente de su hecho en forma plena.[47]

La idea central por la que se recurre a la coautoría en cierta parte de la doctrina que trabaja la problemática de emprendimientos organizacionales de los que derivan hechos ilícitos, tiene que ver con la consideración de que las actividades llevadas a cabo bajo el halo de una

47. Bolea Bardon, Carolina, *Autoría mediata en derecho penal*, Valencia, Tirant Lo Blanch, 2000, p. 358.

empresa u organización con diversas jerarquías y responsabilidades escalonadas, brindan una explicación menos conflictiva con el principio de autorresponsabilidad, si se entiende que existió dominio del hecho compartido entre quienes dirigen y quienes ejecutan, que si se piensa en la subordinación de los ejecutores.

El problema es que la coautoría supone resolución común, que es algo más que la mera pertenencia a una organización, porque la existencia de una resolución común contraviene el orden jerárquico de ordenar y ejecutar lo ordenado. Además, la coautoría se basa en la necesidad de constatar la ejecución conjunta del hecho, por lo que las contribuciones deben llevarse a cabo en el estadio de la ejecución, de manera que la distribución del trabajo debe limitarse a la fase de ejecución.[48]

Para Roxin entonces, un juicio que establezca coautoría provocaría la falsa impresión de que quienes intervienen en distintos niveles tienen la misma responsabilidad por el hecho. Esa falsa impresión que propone la equiparación normativa del "hecho de todos" de Jakobs, ciertamente homogeneiza las intervenciones, precariza la importancia del conocimiento de los hechos y hasta un punto prescinde de ellos.

El asunto es que Jakobs descree de la autoría mediata al desechar el concepto de automatismo y la fungibilidad o intercambiabilidad. Entiende que un dominio superior sólo se justifica si el ejecutor estuviera subordinado jurídicamente al que dicta las órdenes, porque si el ejecutor actúa de forma plenamente responsable, a su entender, no existe jurídicamente ninguna superioridad del que imparte la orden.[49]

Según Bolea Bardon, para entender la autoría de los hombres de atrás, hay que atender al elemento subordinación. Se trata de "Poder de mando, por un lado, y relación de subordinación por el otro, que derivan de una estructura jerárquica, en concreto, de una estructura vertical o piramidal y no de una estructura horizontal".[50]

La crítica de Murmann es clara, pues en esta discusión sobre autoría mediata o coautoría, al hombre de adelante por un lado se lo ve libre y responsable de su hecho y por el otro se lo ve como mero ins-

48. Roxin, Claus, *Täterschaft und Tatherrschaft*, 6ta edición, 1994, p. 280.
49. Jakobs, Günther, "Entscheidungen-Strafrecht", BGH, *NStz*, 1995, p. 27.
50. Bolea Bardon, Carolina, *op. cit.*, p. 397.

trumento del hombre de atrás que domina el suceso por encima del hombre de adelante.[51]

Ambas calidades no pueden ser aplicadas, pues o se es responsable como autor directo que decide o se es instrumento que obra por error o coacción o como una pieza fungible de un entramado de poder que decide sobre los resultados del emprendimiento criminal. O se es una cosa o se es otra, de lo contrario se vulnera un principio básico de lógica formal, me refiero al principio de no-contradicción, que simplemente prescribe que algo no puede ser y no ser al mismo tiempo, y al que los abogados deberíamos recurrir más a menudo para ahorrarnos tiempos de litigio argumental abstracto.

Lo cierto es que en materia de sistemas autónomos, la dogmática se enfrenta a la discusión sobre la capacidad de conducta de una persona jurídica digital o robótica –en este último caso si posee soporte físico de actuación como en el caso de robots bélicos, drones o vehículos autónomos–. Una vez más entonces, la construcción del concepto de "dominio funcional" entre quien ordena y quien ejecuta, supone que en estos casos se tratará de un ser humano quien ordena y un sistema autónomo quien ejecuta.

Desde este aspecto tenemos variantes de análisis. Ninguna duda cabe que si el sistema que ejecuta no tiene capacidad de decisión autónoma, se tratará de un caso de instrumento y quien programe o codifique la acción será autor directo.

El análisis debe sopesar aquellos sistemas que bajo la tecnología de *deep learning* adoptan decisiones basadas en su experiencia y cálculo, y su sofisticación alcanza grados respecto de los cuales no es posible efectuar la trazabilidad de la etiología del proceso decisional. En estos casos, donde detrás de un sistema IA hay una persona a la cual es posible conectar causalmente al diseño, programación, fabricación y puesta en circulación del sistema, habrá que analizar la responsabilidad sobre el resultado ejecutado por el sistema IA sobre dos esquemas.

Uno finalista ontológico, donde la persona y la conducta tiene anclaje en elementos de la realidad y el comportamiento hecho del proceso sólo puede ser efectuado por una persona humana y por lo que los entes jurídicos no tienen capacidad de acción; y otro funcionalista normativo,

51. Murmann, Uwe, *Täterschaft durch weisungsmacht*, GA, 1996, p. 272.

donde la acción en términos jurídicos penales es definida desde el propio ámbito de las normas, la conducta es definida en función de expectativas o roles respecto de lo que la sociedad esperaba del sujeto en el ámbito de sus competencias y en razón de la organización de esfera de responsabilidades en el medio social y así también los sujetos capaces de conducta, tales como las personas jurídicas –empresas–, digitales o robóticas.

Las derivaciones de un ingenio tecnológico plantean diversas posibilidades: a) resultado lesivo por errores de programación que permiten acciones inesperadas; b) resultado lesivo por programación deliberada para que ese hecho ocurra; y c) resultado lesivo ante la actuación de un sistema respecto del cual no es posible prever ni programar su evitación.

Para pensar en responsabilidad penal de la IA, resulta determinante entonces la asignación o calificación de persona jurídica digital o robótica, si posee capacidad acción en términos jurídico-penales y si es pasible de recibir una sanción penal en términos de reproche o si es necesario implementar una penología que incorpore diversas alternativas tales como la intervención Estatal, confiscación, obligación de abrir los códigos de programación y toda aquella información que pese a ser propiedad privada y sujeta a derechos de propiedad intelectual, patentes o autor, pierda el privilegio cuando el sistema autónomo afecte la dignidad, vida, libertad, integridad, privacidad y propiedad del ser humano.[52]

Una vez ello, también será determinante para el análisis el marco de codificación y los recaudos empleados para eliminar los riesgos derivados de la actuación del sistema autónomo.

52. Baigún propuso penas para las personas jurídicas que básicamente se reducen a la cancelación de la personería jurídica, multa, suspensión total o parcial de actividades, clausura de alguno de sus establecimientos, pérdida de beneficios estatales, prohibición de actuar en el mercado por un tiempo determinado, publicidad de la sentencia condenatoria, y también la creación de un consejo de vigilancia en la empresa para control durante un lapso de tiempo.
El artículo 68 del Anteproyecto de reforma del Código Penal preveía la imposición de sanciones consistentes en multa limitada, cancelación de la personería jurídica, clausura total o parcial de hasta tres años, pérdida o suspensión de beneficios estatales, publicación de la sentencia condenatoria a su costa, prestaciones obligatorias vinculadas al daño ocasionado, comiso, intervención judicial de hasta tres años, auditoria periódica, suspensión de uso de patentes y marcas de hasta tres años y suspensión de hasta tres años en los registros de proveedores del Estado, a los entes de existencia ideal en cuyo nombre, representación, interés o beneficio hubieran actuado los sujetos intervinientes en el hecho.

En palabras del Parlamento Europeo, la identificación de las responsabilidades últimas de los sujetos humanos detrás del desarrollo tecnológico, deben analizarse en función del

> ... nivel real de las instrucciones impartidas [...] y a su grado de autonomía, de forma que cuanto mayor sea la capacidad de aprendizaje o la autonomía y cuanto más larga haya sido la formación del [sistema IA], mayor debiera ser la responsabilidad de su formador...[53]

El código fuente o la programación base que brinde un marco de instrucciones amplio, con mayor autonomía del sistema para la determinación conductual, distanciará la responsabilidad directa intencional del sujeto humano, conjunto de personas o empresa, autor de la programación.

El hecho objeto de estudio penal, la acción o hecho ejecutado por el sistema autónomo, puede no formar parte de la codificación inicial. En este caso habrá situaciones de previsibilidad que habrá que tomar en cuenta e incluso la posibilidad de considerar al sistema un instrumento mediante el cual es posible la ejecución de un comportamiento desde el punto de vista causal, que es imputable y atribuible en función de la programación defectuosa del obrar y la posición de garantía respecto de las acciones posibles del sistema y de allí el abordaje desde títulos imprudentes.

Un marco de instrucciones cerrado, vincula más estrechamente la responsabilidad por resultados que se encuentren dentro del ámbito esperable de actuación del sistema.

Bajo estos cánones, aproximar los instrumentos dogmáticos del derecho penal, a efectos de intentar regular una materia dinámica y de difícil abordaje con herramientas fundadas para contemplar acciones humanas en un medio escasamente interferido por la tecnología, se torna complejo y termina por expandir la aplicación de la ley con una hermenéutica que la hace porosa, cuestionable por su intento de acaparar un universo de supuestos que se encuentran fuera de su horizonte natural de aplicación.

Lo cierto es que la discusión central de la actualidad es el debate sobre el estatus ontológico que puede adquirir el nacimiento de una

53. Texto aprobado con fecha 16 de febrero de 2017 –P8_TA(2017)0051–, pto. 56 del documento.

tecnología que tenga la capacidad de adquirir capacidad de decisión y en cierta manera, consciencia de su existencia, del medio y aspectos abstractos y complejos que emparenten sus mecanismos de reflexión de manera que sea difícil distanciarlos del ser humano en ese tópico.

Allí está la discusión sobre la necesidad de prever una solución jurídica nueva y distinta –ciberderecho, *lex* robótica, derecho de la IA, etc.–, siendo sustancial en el ámbito del derecho penal el principio de autorresponsabilidad.[54]

Como vengo exponiendo, el mismo problema del estatus ontológico de la IA, lo recibe la persona jurídica o empresa a la que se le adjudica con la legislación reciente capacidad de acción, posibilidad de estar en juicio y recibir penas. El problema sobre el principio de autorresponsabilidad aquí, como señala Quintero Olivares, se da con un obstáculo vinculado a la condición ontológica que caracteriza al derecho penal en cuanto a que sus posibles reacciones sean conocidas *ex ante* por los hipotéticos futuros trasgresores, lo que supone un derecho previamente conocido.[55]

En este sentido, se verá en lo que sigue cuál es el núcleo de imputación que se ha previsto en la materia para las personas jurídicas y qué papel juega el principio de precaución en derecho medioambiental.

Compliance y principio de precaución

Como señala Yacobucci, diversos casos en el ámbito angloamericano han servido de base a distintas regulaciones que precisamente son las que inspiraron las disposiciones de la ley penal de la empresa dictada en nuestro ordenamiento –Ley N° 27401–.[56]

54. Ver en este sentido, Sánchez del Campo Redonet, "Cuestiones jurídicas que plantean los robots", en *Revista de privacidad y derecho digital*, N° 2, 2016; y así también, *Reflexiones de un replicante legal*, Aranzadi, 2016.

55. Quintero Olivares, Gonzalo, "La robótica ante el derecho penal: el vacío de respuesta jurídica a las desviaciones incontroladas", en *Revista de Estudios Penales y de la seguridad*, 1, 2017. Disponible en: www.ejc-reeps.com

56. Yacobucci, Guillermo J., *op. cit.*, p. 6, donde sostiene que "Los casos 'Boeing', 'Parmalat' pero, sobre todo, 'Enron' y, poco después, 'Lehman', han obrado en el ámbito angloamericano como disparadores, respectivamente, de reacciones legislativas de enorme importancia. El acta Sarbanes-Oxley –2002– y, más tarde, el acta Dodd-Frank –2010– han constituido directrices que se han visto reflejadas, por un lado, en

Esa compilación de deberes de previsión y regulación de estructuras dinámicas, han tenido en vista la creación de acciones, mecanismos, programas y procedimientos, para el control y supervisión, con el objeto de prevenir, detectar y corregir irregularidades y actos ilícitos derivados de la actividad. Si bien se trata de estructuras necesarias para el desarrollo en sociedad, deben encontrar límite de contención de los riesgos intrínsecos que conllevan.

En materia de IA, en todos los escenarios en donde se funde esta tecnología y se hace cada día más presente, existe la necesidad de, en palabras del Parlamento Europeo, basar los desarrollos tecnológicos en la interdependencia, previsibilidad y direccionalidad de la innovación (ptos. 50 y 51 del documento).[57]

La gestión de riesgos debía estar signada por la posibilidad efectiva de minimizarlos y neutralizar el impacto negativo de la innovación que a su vez debe estar regida por el principio de precaución, de manera de supervisar la transición de la sociedad hacia tecnologías sobre las que deberá efectuarse evaluación constante de seguridad (ptos. 6, 7, 54 y 55 del documento citado).

El principio de precaución se origina en los setenta en Alemania, se expande en los años ochenta en diversas legislaciones y su formulación internacional más clara surge de la Declaración de Río de Janeiro de 1992 sobre el Medio Ambiente y el Desarrollo, al establecer en el Principio 15 que

> ... con el fin de proteger el medio ambiente, los Estados deberán aplicar ampliamente el criterio de precaución conforme a sus capacidades. Cuando haya peligro de daño grave o irreversible, la falta de certeza científica absoluta no deberá utilizarse como razón para postergar la adopción de medidas eficaces en función de los costos para impedir la degradación del medio ambiente.

Como señala Susana Escobar Vélez, en el Protocolo de Cartagena sobre Seguridad de la Biotecnología se consolidó el "enfoque de precaución" contenido en la Declaración de Río, y en el artículo 10.6 otorgó la facultad de adoptar una decisión con respecto a la importación

las *Federal Sentencing Guidelines* (FSG) (1) –especialmente en el capítulo ocho– y, por el otro, en las regulaciones de la Security and Exchange Commission (SEC)".

57. Texto aprobado con fecha 16/02/2017 –P8_TA(2017)0051–.

de organismos vivos modificados (en el sentido de prohibir esta o solicitar información adicional) aunque no se tuviera "certeza científica por falta de información o conocimientos científicos pertinentes suficientes sobre la magnitud de los posibles efectos adversos" de dichos organismos. En síntesis, para estas formulaciones, el principio de precaución se traduce en "decidir adoptar medidas sin esperar a disponer de todos los conocimientos científicos necesarios".[58]

La sustancia entonces del principio de precaución se ciñe a la adopción de medidas sin esperar a disponer de todos los conocimientos científicos necesarios, de manera de prevenir riesgos de la utilización de determinadas prácticas o innovaciones de las que no sea posible calcular ni evaluar el impacto en la sociedad.

En materia de IA, la ciencia hoy día no es capaz de prever todas las derivaciones de los desarrollos en este campo, de manera de ser imposible afirmar que no ocurrirá ningún resultado dañoso singular o de escala.

Pareciera entonces que la inclusión del principio de precaución al derecho penal, sin ninguna textura especial ni consideración en particular, significaría trasladar principios del campo administrativo a las reglas de debido cuidado que supondrían ampliar el espectro del controvertido estándar de los delitos de peligro abstracto.

Se critica que el principio de precaución no sirve para explicar los delitos de peligro, ni los imprudentes, ni puede constituirse en una explicación alternativa de un estatus delictivo nuevo.[59]

Lo cierto es que en materia de delitos imprudentes, la noción de riesgo permitido encuentra relación clara con los riesgos derivados de los avances tecnológicos, cuya innovación tiende a mejorar la vida por definición. La aceptación de esta directriz contiene la idea de la aceptación de determinados riesgos de la innovación, pues de lo contrario la expansión de la precaución paralizaría los desarrollos y descubrimientos en el campo científico.

Si bien es cierto que el criterio que se desprende del principio analizado impone un desconocimiento de las consecuencias posibles de la innovación, su enfoque preventivo debe estar acompañado de pará-

58. Escobar Vélez, Susana, "El traslado del principio de precaución al derecho penal en España", en *Revista Nuevo Foro Penal*, Vol. 6, N° 75, julio-diciembre 2010, Universidad EAFIT, Medellín, pp. 15-40.

59. Quintero Olivares, Gonzalo, *op. cit.*, p. 21.

metros objetivos que restrinjan de modo preciso y calculable el ámbito de lo esperable por los operadores en el campo de la IA, de manera de cumplimentar el espíritu que el principio trae al derecho penal desde su natural ámbito del derecho medioambiental.

En este marco, la idea de identificar las cadenas de responsabilidad en el campo de la IA, de todos los intervinientes que tienen injerencia de manera individual o colectiva en el desarrollo de nuevas tecnologías bajo presupuestos de matrices de pensamiento que contienen un elevado nivel decisional de imposible trazabilidad, supone asignar con fines precautorios, todo un cuerpo de planes y programas integrales que promuevan las acciones dirigidas a neutralizar riesgos no aceptables, y acoten las irregularidades y desvíos que deriven en resultados de contenido ilícito.

Los planes de integridad del ámbito de la persona jurídica, sirven de base para generar un ámbito de "*compliance* digital", donde los cuerpos éticos, códigos de conducta, códigos deontológicos, autorregulaciones, licencias de producción, comercialización y uso, deberán contener legislaciones que junto al concepto precautorio derivado de este principio, permitirán adecuar un derecho penal más racional a la regulación de los hechos derivados de la interacción que provocarán las más avanzadas tecnologías con IA en la sociedad.

En este punto, ya sea desde un sistema de imputación ontológico con aceptación de un esquema de doble jurisdicción y la posibilidad de incorporar sanciones administrativas, o desde un sistema normativo con la autodefinición de conceptos desde el ámbito de las normas y la posibilidad de nominar a los entes digitales como personas jurídicas digitales o robóticas, con un esquema de imputación unidireccional, resultará clave la implementación de pautas objetivas derivadas de exigencias reglamentarias de la actividad científica y la innovación en materia de tecnologías de aprendizaje profundo, donde la decisión del sistema autónomo no sea pasible de trazabilidad y la etiología de la decisión deba atribuirse en función de un tamiz construido y constituido por la *compliance* digital.

En definitiva, se trata de asignar competencia bajo esquemas de posiciones de garantía de desarrolladores, *productores*, comerciantes, usuarios y Estado, respecto de la intervención de sistemas autónomos en hechos delictivos.

Esta aproximación al derecho penal de la inteligencia artificial tiene en vista también la posibilidad de incorporar a los planes de precaución, principios tales como los derivados de las Leyes de Asimov,[60] que como ha señalado el estudio del comité jurídico del Parlamento Europeo,[61] deben considerarse dirigidos a diseñadores, productores y operadores en la materia, preservando la coexistencia pacífica o, como también ha señalado el comité, de conjunta acción.

Relevancia de la persona jurídica digital y conclusión

Podríamos preguntarnos por qué la figura de la persona jurídica a secas no podría ser introducida en el ámbito de los entes autónomos digitales o mecánicos a los mismos fines que en el ámbito de la empresa. Podríamos preguntarnos cuál es la diferencia o necesidad de introducir una categoría propia, una *lex* robótica.

En principio, el estatus ontológico que adquirió la empresa a través de la legislación comentada en este artículo, es el mismo que tendría la persona jurídica digital. En lo particular, la necesidad de concretizar una rama específica que contemple el derecho de los sistemas autónomos digitales o robóticos, se origina en la caracterización que la tecnología que rodea a los avances en materia de sistemas autónomos tiene. El estudio de todos los aspectos que hacen a la intervención de sistemas autónomos, responsables penalmente bajo esquemas de doble jurisdicción o imputación directa de corte normativo, debe contemplar aspectos específicos que hacen a la injerencia comportamental que tendrán estos entes.

En este lineamiento, la infinidad de interacciones provocadas por los incontables sistemas que actuarán en diferentes áreas y aspectos de la vida cotidiana, hace necesario pensar rasgos específicos para las

60. Ver Asimov, Isaac, "Círculo vicioso" (*Runaround*, 1942): "1- Un robot no hará daño a un ser humano o, por inacción, permitir que un ser humano sufra daño. 2- Un robot debe cumplir las órdenes dadas por los seres humanos, a excepción de aquellas que entrasen en conflicto con la primera ley. 3- Un robot debe proteger su propia existencia en la medida en que esta protección no entre en conflicto con la primera o con la segunda ley". Y la Ley Zero, escrita por el autor 40 años después, "Un robot no puede causar daño a la humanidad o, por inacción, permitir que la humanidad sufra daño".

61. European civil law rules in robotics (Normas europeas de Derecho Civil sobre robótica), PE 571.379. Manuscrito completado en octubre de 2016. © Unión Europea, 2016.

definiciones del ámbito de lo permitido en este campo, los roles de cada actor del largo segmento de responsables en su puesta en funcionamiento, y las exigencias previsibilidad y direccionalidad de los proyectos e innovaciones en la industria digital.

Los controles sobre la trazabilidad añorada no sólo del proceso decisional, sino también de los contenidos registrados por el ente o sistema autónomo y de la competencia de cada responsable en el rol que tenga en el entramado referido, desde el diseñador hasta el usuario y el Estado como controlador y garante de la minimización de los riesgos de la innovación bajo el principio de precaución, son los que evidencian la necesidad de mecanismos legales propios de una especialidad jurídica abocada a este campo.

A modo conclusivo, me permito finalizar este documento con una breve reflexión.

Con la responsabilidad penal de la empresa en nuestro medio renació una discusión con contenido dogmático y político criminal en el ámbito del derecho penal. Parafraseando al profesor Yacobucci, a pesar de sus reservas personales con el principio de culpabilidad en este asunto, el contenido material de la responsabilidad de la persona jurídica reside en los defectos de configuración de su cultura ética. Esta falla de configuración se identificó en la ausencia de sistemas de controles y supervisión como trazo integral de la persona jurídica.

Necesariamente los avances científicos en este campo nos acercarán cada día más a la temida singularidad tecnológica, signada por el día en el que los entes computacionales revelarán sus propias creaciones, que bajo el don de las operaciones sintéticas escalonadas por la superioridad de procesamiento, provocarán un mejor resultado que el que se encuentre al alcance de la biología humana. Bajo este aspecto, la aspiración de los debates parlamentarios en los diversos comités de legislación citados en este trabajo, tienen en consideración –muchas veces con temor–, a los riesgos y las implicancias de la pérdida del control sobre las nuevas tecnologías autónomas.

Comparativamente es posible afirmar que el núcleo de responsabilidad penal de la persona jurídica digital o robótica está dado por los defectos de configuración y desarrollo de la individualidad del ente ante un principio de coexistencia que tiende, a mi juicio, a una justa reformulación de la Ley Zero de Asimov. En efecto, que toda inteligencia

artificial debe desarrollarse sin agredir la dignidad, libertad y vida humanas, preservando la coexistencia.

Parece claro aquí que la importancia de una categoría de estudio específico, tanto desde la filosofía, ética y derecho, para una era digital, es un imperativo categórico.

Bibliografía

AMBOS, Kai, "Dogmática jurídico-penal y concepto universal de hecho punible", en *Política Criminal*, Vol. 3, N° 5, 2008, A6-5; con cita de GIMBERNAT, Enrique, "Hat die Strafrechtsdogmatik eine Zukunft?", ZStW. 82 (1970).

ASIMOV, Isaac, "Círculo vicioso" (*Runaround*, 1942).

BOLEA BARDON, Carolina, *Autoría mediata en derecho penal*, Valencia, Tirant Lo Blanch, 2000.

CASTEX, Francisco (dir.); DUBINSKI, Andrés M. y MARTÍNEZ, Sebastián (coords.), *Responsabilidad Penal de la Persona Jurídica y Compliance*, Buenos Aires, Ed. Ad-Hoc, 2018.

CEREZO MIR, José, *Derecho Penal. Parte General*, Buenos Aires, Ed. BdeF, 2008.

ESCOBAR VÉLEZ, Susana, "El traslado del principio de precaución al Derecho penal en España", en *Revista Nuevo Foro Penal*, Vol. 6, N° 75, Universidad EAFIT, Medellín, julio-diciembre de 2010.

GIMBERNAT ORDEIG, Enrique, *Autor y cómplice en derecho penal*, Buenos Aires, Ed. BdeF, 2006.

JAKOBS, Günther, "El ocaso del dominio del hecho. Una contribución a la normativización de los conceptos jurídicos", en *Dogmática y política criminal en una teoría funcional del delito* (trad. de Manuel Cancio Meliá), Buenos Aires, Rubinzal-Culzoni Editores, 2000.

_____, Entscheidungen-Strafrecht, BGH, *NStz*, 1995.

MURMANN, Uwe, *Täterschaft durch weisungsmacht*, GA, 1996.

QUINTERO OLIVARES, Gonzalo, "La robótica ante el derecho penal: el vacío de respuesta jurídica a las desviaciones incontroladas", *Revista de Estudios Penales y de la seguridad*, N° 1, 2017. Disponible en: www.ejc-reeps.com

REYES ALVARADO, Yesid, "El concepto de imputación objetiva", en *El Derecho Penal Contemporáneo*, Nº 1, Ed. Legis, octubre de 2002.

ROXIN, Claus, *Derecho Penal. Parte General*, Buenos Aires, Ed. Thomson Reuters-Civitas, 2014.

SCHÜNEMANN, Bernd, *Obras*, Santa Fe, Rubinzal-Culzoni, T. I, 2009.

VOLK, Klaus, *La verdad sobre la verdad y otros estudios*, Buenos Aires, Ed. Ad-Hoc, 2007.

YACOBUCCI, Guillermo J., "La empresa como sujeto de imputación penal", en *La Ley*, año LXXXI, N° 225, 2017.

ZAFFARONI, Eugenio R.; ALAGIA, Alejandro y SLOKAR, Alejandro, *Manual de Derecho Penal. Parte General*, Buenos Aires, Ed. Ediar, 2ª edición, 2002.

La protección de los derechos de niñas, niños y adolescentes frente al delito de *grooming*

Yael Bendel*

Introducción

El presente artículo tiene como finalidad introducirnos en la problemática del *grooming*, su vinculación con las obligaciones asumidas en torno a la protección de niñas, niños y adolescentes y con el concepto de corresponsabilidad, enmarcado este dentro del sistema de protección de derechos.

Grooming es un término anglosajón que está relacionado con "la preparación para algo" (*groom:* "acicalar"). Este delito inició su desarrollo legislativo en los países del Common Law,[1] y se extendió posteriormente por varios países. Se lo define como el proceso por el cual un adulto contacta a una niña, niño o adolescente a través del uso de medios digitales (aplicaciones, juegos en línea, redes sociales, mensajería, etc.) para ganar su confianza, con el propósito de captarlo y controlarlo con fines sexuales.

En la era digital las prácticas consistentes en conductas sexuales agresivas contra niñas, niños y adolescentes han evolucionado: los agresores logran permanecer en el anonimato y perseguir un mayor número de víctimas haciendo uso de Internet. Las nuevas tecnologías generan una mayor oportunidad para tales formas comunes de delincuencia contra los niños y niñas,[2] motivo por el cual los Estados deben avanzar en nuevas formas de protección.

* Abogada egresada de la UBA. Asesora General Tutelar del Poder Judicial de la Ciudad Autónoma de Buenos Aires.

1. Es el derecho común o derecho consuetudinario vigente en la mayoría de los países de tradición anglosajona. En dichos países se denomina también *"child grooming"*.

2. Oficina de Naciones Unidas contra la Droga y el Delito, "Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children", UNODC,

Es pertinente reconocer que el deber de proteger a niñas, niños y adolescentes y de garantizar su derecho a la integridad y a la seguridad digital surge de preceptos supranacionales receptados por la Constitución Nacional, que obligan al Estado, a la familia y a la sociedad a brindarles un plus de protección.

En este artículo recordaremos el predominio rector sobre los derechos humanos de niñas, niños y adolescentes, para luego detenernos en la definición del delito de *grooming*.

Introduciremos algunas de las características de la población víctima del delito de *grooming*, y nos referiremos a la corresponsabilidad como punto de partida de los deberes de protección integral.

Por último, ensayaremos algunas ideas y sugerencias a fin de generar preguntas y vislumbrar respuestas positivas para garantizar los derechos de niñas, niños y adolescentes.

La supremacía de los derechos de niñas, niños y adolescentes

El derecho internacional comenzó a transitar el reconocimiento de niñas, niños y adolescentes a fines del siglo XIX. A principios del siglo XX, en Europa, se realizaron los primeros congresos sobre la temática que se extendieron luego al continente americano.[3] Primariamente tuvieron un componente benefactor y altruista, hasta que finalmente alcanzaron una "perspectiva de derechos".

Podemos afirmar que la historia de la infancia transitó tres momentos principales: el de la invisibilización de las niñas y niños, el de su concepción como objetos o menores incapaces, y el de su reconocimiento como sujetos plenos de derechos.

Luego de recorrer un dificultoso camino hacia el reconocimiento de las niñas y niños como sujetos plenos de derechos, se proclamó

Viena, mayo de 2015. Disponible en: https://www.unodc.org/documents/commissions/CCPCJ/CCPCJ_Sessions/CCPCJ_23/E-CN15-2014-CRP1_E.pdf

3. París 1905; Bruselas 1907; Washington 1909 y Buenos Aires 1910. Para más información ver Iglesias, Susana; Villagra, Helena y Barrios, Luis, "Un viaje a través de los espejos de los congresos panamericanos de niños", en AA. VV., *Del revés al derecho. La condición de la infancia en América Latina. Bases para una reforma legislativa*, Buenos Aires, Galerna/UNICEF/UNICRI/ILANUD.

la Convención Internacional sobre los Derechos del Niño (CIDN),[4] "inscribiéndose en la corriente más universal de la garantía y la protección de los derechos humanos".[5]

La CIDN es un pacto de derechos humanos de la infancia, que abarca derechos sociales, económicos, culturales, civiles y políticos; y ha sido universalmente reconocida y ratificada por países de todos los continentes.[6]

La República Argentina la incorporó a su ordenamiento jurídico interno en el año 1990, a través de la Ley N° 23849. En 1994, con motivo de la reforma convencional, se le otorgó jerarquía constitucional a través de su incorporación a la Carta Magna (art. 75, inc. 22).

La Convención, como tratado de derechos humanos para la infancia basado en la teoría de la protección integral, contiene principios[7] que obligan a los Estados a diseñar políticas públicas dirigidas a satisfacer los principios de interés superior del niño,[8] desarrollo integral,[9]

4. Resolución N° 44/1925 adoptada por la Asamblea General de las Naciones Unidas el 20 de noviembre de 1989 en Nueva York.

5. Cillero Bruñol, Miguel, "Infancia, Autonomía y Derechos: una cuestión de principios", en *Infancia*, Boletín del Instituto Interamericano del Niño N° 234.

6. Estados Unidos es el único país que no ratificó la CIDN. La suscribió, pero no depositó el instrumento de ratificación.

7. UNICEF. "Derechos bajo la Convención de los Derechos del Niño". Disponible en: https://www.unicef.org/spanish/crc/index_30177.html [Fecha de consulta del 20/02/2011].

8. Artículo 3 CIDN: "En todas las medidas concernientes a los niños que tomen las instituciones públicas o privadas de bienestar social, los tribunales, las autoridades administrativas o los órganos legislativos, una consideración primordial a que se atenderá será el interés superior del niño. Los Estados Partes se comprometen a asegurar al niño la protección y el cuidado que sean necesarios para su bienestar, teniendo en cuenta los derechos y deberes de sus padres, tutores u otras personas responsables de él ante la ley y, con ese fin, tomarán todas las medidas legislativas y administrativas adecuadas. Los Estados Partes se asegurarán de que las instituciones, servicios y establecimientos encargados del cuidado o la protección de los niños cumplan las normas establecidas por las autoridades competentes, especialmente en materia de seguridad, sanidad, número y competencia de su personal, así como en relación con la existencia de una supervisión adecuada".

9. El principio de desarrollo integral del niño se ve reflejado en todo el articulado de la CIDN. El Comité de los Derechos del Niño, en su Observación General N° 5 ("Medidas Generales de Aplicación de la Convención sobre los Derechos del Niño, CRC/GC/2003, 5) interpreta el término desarrollo en su sentido más amplio, como concepto holístico que abarca el desarrollo físico, mental, espiritual, moral, psicológico y social de un niño.

igualdad y no discriminación,[10] prioridad en el diseño de políticas públicas (pro niño), centralidad en la familia,[11] y el derecho a ser oído[12] y a la participación y autonomía progresiva, entre otros, que obligan a los poderes de los Estados nacional y provinciales a trabajar en consonancia con el respeto, la promoción, la protección y la restitución de los derechos de niñas, niños y adolescentes.

En lo que respecta a la protección contra toda forma de abuso, la Convención estableció la prohibición absoluta de toda forma de maltrato infantil, de abuso y de explotación sexual,[13] y obligó a los Estados parte a crear políticas públicas apropiadas para garantizar los derechos de las niñas y los niños.

10. Artículo 2.1 CIDN: "Los Estados Partes respetarán los derechos enunciados en la presente Convención y asegurarán su aplicación a cada niño sujeto a su jurisdicción, sin distinción alguna, independientemente de la raza, el color, el sexo, el idioma, la religión, la opinión política o de otra índole, el origen nacional, étnico o social, la posición económica, los impedimentos físicos, el nacimiento o cualquier otra condición del niño, de sus padres o de sus representantes legales".

11. Arts. 5 y 9.

12. Art. 12 CIDN: "Los Estados Partes garantizarán al niño que esté en condiciones de formarse un juicio propio el derecho de expresar su opinión libremente en todos los asuntos que afectan al niño, teniéndose debidamente en cuenta las opiniones del niño, en función de la edad y madurez del niño. Con tal fin, se dará en particular al niño oportunidad de ser escuchado, en todo procedimiento judicial o administrativo que afecte al niño, ya sea directamente o por medio de un representante o de un órgano apropiado, en consonancia con las normas de procedimiento de la ley nacional".

13. Art. 19 CIDN: "Los Estados Partes adoptarán todas las medidas legislativas, administrativas, sociales y educativas apropiadas para proteger al niño contra toda forma de perjuicio o abuso psicológico mental, descuido o trato negligente, malos tratos o explotación, incluido el abuso sexual, mientras el niño se encuentre bajo la custodia de los padres, de un representante legal o de cualquier otra persona que lo tenga a su cargo. Esas medidas de protección deberían comprender, según corresponda, procedimientos eficaces para el establecimiento de programas sociales con objeto de proporcionar la asistencia necesaria al niño y a quienes cuidan de él, así como para otras formas de prevención y para la identificación, notificación, remisión a una institución, investigación, tratamiento y observación ulterior de los casos antes descritos de malos tratos al niño y, según corresponda, la intervención judicial".
Artículo 34 CIDN: "Los Estados Partes se comprometen a proteger al niño contra todas las formas de explotación y abuso sexuales. Con este fin, los Estados Partes tomarán, en particular, todas las medidas de carácter nacional, bilateral y multilateral que sean necesarias para impedir: La incitación o la coacción para que un niño se dedique a cualquier actividad sexual ilegal; La explotación del niño en la prostitución u otras prácticas sexuales ilegales; La explotación del niño en espectáculos o materiales pornográficos".

Hasta aquí, podemos afirmar que las niñas, niños y adolescentes detentan derechos supranacionales, producto de un específico e internacional movimiento de derechos humanos de la infancia que conminó a los Estados a garantizar sus derechos de modo prioritario. Ello implica no sólo la obligación estatal que tiene Argentina de reconocer y respetar dichos derechos sino, principalmente, la obligación constitucional de los tres poderes del Estado de crear programas de promoción de derechos, así como de prevención, persecución y castigo de delitos contra niñas, niños y adolescentes, atendiendo a las nuevas modalidades delictivas en torno a los avances de la tecnología.

El delito de *grooming*

El *grooming* tiene como característica principal el propósito sexual, logrado por medio de acciones premeditadas por parte de un adulto, tendientes a generar un vínculo emocional con la niña, niño o adolescente.[14]

En primer lugar, fue legislado en los países del *common law*, donde ha sido definido como *preying sexually on a child*, cuya traducción literal sería "cazando sexualmente a un niño", en el sentido de aprovecharse de niñas, niños y adolescentes con fines sexuales.

La aprobación del "Convenio del Consejo de Europa para la Protección de los Niños contra la Explotación y el Abuso Sexual" (25/10/2007) motivó que muchos países europeos incluyan en su legislación interna el delito de *grooming*, a partir de receptar el artículo 23 del Convenio, que establece:

> Cada Parte adoptará las medidas legislativas o de otro tipo que sean necesarias para tipificar como delito el hecho de que un adulto, mediante las tecnologías de la información y la comunicación, proponga un encuentro a un niño que no haya alcanzado la edad fijada en aplicación del

14. Al respecto se ha sostenido que "el *grooming* engloba a todas aquellas prácticas *online* que realizan adultos con ciertas patologías que en la jerga internauta son conocidos como *groomer* para ganarse la confianza de un menor, fingiendo empatía, cariño, etc. normalmente bajo una falsa identidad de otro/a menor (conocido o no de la víctima), con la finalidad de satisfacer sus apetencias sexuales. Vaninetti, Hugo, "Inclusión del *grooming* en el Código Penal", *La Ley* 2013-F-1200, 16/12/2013.

> apartado 2[15] del artículo 18 con el propósito de cometer contra él cualquiera de los delitos tipificados con arreglo del apartado 1[16] del artículo 18 o al apartado a)[17] del artículo 20, cuando a dicha proposición le hayan seguido actos materiales conducentes a dicho encuentro.

Los Estados miembros del Consejo de Europa impulsaron la firma de este instrumento internacional motivados por la creciente preocupación que les generaba la expansión de los delitos de explotación y abuso sexual contra niños y niñas, con especial énfasis en la dimensión adquirida a través del uso que los niños y niñas realizan en forma autónoma de las nuevas tecnologías, y la consecuente exposición que esto conlleva.

La globalización y la masificación en el uso de las nuevas tecnologías propició enormes beneficios, pero también riesgos, ya que antiguas modalidades delictivas mutaron, se adaptaron y encontraron un mayor caudal de "posibles víctimas", así como posibilidades de nuevas formas de engaño y anonimato en las redes.

En la República Argentina, el delito de *grooming* fue incorporado al Código Penal Argentino en el año 2013, a través de la inclusión del artículo 131.[18] Dicho artículo establece que

> Será penado con prisión de seis (6) meses a cuatro (4) años el que, por medio de comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos, contactare a una persona menor de edad, con el propósito de cometer cualquier delito contra la integridad sexual de la misma.

Con relación al bien jurídico tutelado, se persigue proteger la integridad sexual de niñas, niños y adolescentes, la cual, como ya observamos, adquiere un plus de protección a través de la amplia normativa supranacional que protege sus derechos.

La figura penal se encuentra dentro del Título III del Código Penal, que a través de la modificación de la Ley N° 25087 adquiere la denominación de "delitos contra la integridad sexual". La integridad sexual ha sido

15. Cada Estado determinará la edad por debajo de la cual no está permitido realizar actividades sexuales con niños.

16. Actividades tipificadas como abuso sexual hacia niñas, niños y adolescentes.

17. Pornografía infantil.

18. Ley N° 26904.

entendida como "el normal ejercicio de la sexualidad, asentada sobre la libertad del individuo".[19] También se la ha definido como

> La libertad sexual de la persona mayor de dieciocho años y el libre desarrollo sexual de los menores de edad, partiendo de la base que nadie puede introducirse en la esfera sexual ajena, sin la voluntad de la otra persona, con capacidad para consentir, y menos aún en quien no lo puede hacer.[20]

Más allá de las discusiones dogmáticas respecto del tipo penal, de su clasificación como delito informático propio o impropio, o de la posible vulneración de garantías constitucionales vinculadas al principio de legalidad y proporcionalidad,[21] que no pretenden ser materia de análisis en este artículo, resulta necesario considerar que no nos debemos apartar de los compromisos internacionales asumidos en torno a la prevención y protección de derechos, así como a la sanción de los delitos contra la integridad sexual que tengan como víctimas a personas menores de edad.

El artículo 131 incorporado al Código Penal puso énfasis en la acción de contactar con fines de afectar la integridad sexual de niñas y niños. La acción de contactar presupone diferentes etapas; primeramente, generar una relación de amistad con el niño o niña fingiendo edad e identidad, para luego obtener información de él o ella. Se suele utilizar la seducción para obtener datos íntimos que permitan la extorsión, para conseguir fotos con contenido sexual (pornografía) y/o un encuentro físico.

El delito de *grooming* si bien utiliza como medio comisivo las nuevas tecnologías, no es más que un desplazamiento de técnicas utilizadas por pedófilos y agresores sexuales, que han encontrado en las aplicaciones, redes sociales y demás plataformas digitales una nueva modalidad para interactuar por medio del engaño con los niños, niñas y adolescentes, que son emisores y receptores de información, nucleados en torno a un "mundo virtual segregado por la comunicación".[22]

---

19. Creus, Carlos y Buompadre, Jorge E., *Derecho penal. Parte especial*, 7ma edición actualizada y ampliada, Buenos Aires, Ed. Astrea, T. I, 2007, p. 180.

20. Donna, Edgardo, *Delitos contra la integridad sexual*, Santa Fe, Rubinzal-Culzoni, 2000.

21. Garibaldi, Gustavo, "Aspectos dogmáticos del *grooming* legislado en Argentina", en *Revista Derecho Penal*, año III, N° 7, mayo de 2014. Disponible en: http://www.saij.gob.ar; Vianna, Tulio, *Fundamentos de Direito Penal Informático*, Río de Janeiro, Editora Forense Jurídica, 2003.

22. Lerma Morón, Esther, *Internet y Derecho Penal: hacking y otras conductas ilícitas en la red*, Navarra, Aranzadi, 2ª ed., 2002, p. 89.

Compromiso y protección con los derechos de niñas, niños y adolescentes

La CIDN establece el sistema de la protección integral, entendido este como la necesidad de que los Estados adopten medidas dirigidas a garantizar el desarrollo integral de niñas, niños y adolescentes, asumiendo el rol de garante de los derechos. Introduce una nueva modalidad de abordaje que requiere no solo una nueva institucionalidad, sino también una nueva organización de trabajo adaptada a los preceptos convencionales, con diversos sectores, nuevos actores, y diferentes niveles de protección.

La Comisión Interamericana de Derechos Humanos señaló que

> ... los Estados deben diseñar sus intervenciones de forma integral, considerando la interconexión y complementariedad de todos los derechos. Además, debe aplicarse un enfoque multifacético que considere: la promoción, difusión y sensibilización sobre derechos de la niñez; la prevención de violaciones; la protección frente a riesgos o injerencias ilegítimas; la restitución de derechos; la reparación y rehabilitación; y, la justicia a través de la investigación, enjuiciamiento y sanción a los responsables de violaciones de derechos.[23]

Por su parte la Ley Nacional N° 26061 de protección integral de los derechos de niñas, niños y adolescentes, instituye el sistema de protección integral nacional, conformado por

> ... todos aquellos organismos, entidades y servicios que diseñan, planifican, coordinan, orientan, ejecutan y supervisan las políticas públicas, de gestión estatal o privadas, en el ámbito nacional, provincial y municipal, destinados a la promoción, prevención, asistencia, protección, resguardo y restablecimiento de los derechos de las niñas, niños y adolescentes.[24]

A nivel local, el sistema de protección de derechos de la Ciudad Autónoma de Buenos Aires[25] es un sistema con enfoque de derechos,

23. Comisión Interamericana de Derechos Humanos, "Hacia la garantía efectiva de los derechos de niñas, niños y adolescentes: Sistemas Nacionales de Protección", (referencia: OEA/Ser. L/V/II.166. Doc. 206/2017).

24. Art. 32, Ley N° 26061.

25. Tiene como marco normativo la CIDN, Ley Nacional de Promoción y Protección Integral N° 26061 y Ley local N° 114 de Protección Integral de los Derechos de Niñas, Niños y Adolescentes de la Ciudad de Buenos Aires.

abordaje integral e intersectorial que respeta el derecho a ser oído y garantiza la participación del niño y la familia en los procedimientos. De estas definiciones se desprende la idea de *corresponsabilidad*, entendida como la obligación de todos los actores gubernamentales y no gubernamentales de implementar acciones de protección de derechos mediante el trabajo articulado, intersectorial y simultáneo.

La familia, la sociedad civil y el Estado son corresponsables de garantizar derechos de niñas, niños y adolescentes, ubicándose este como garante último de estos derechos.

La corresponsabilidad implica que todos los actores tienen la obligación de implementar acciones de promoción y prevención en relación con el delito de *grooming*, como así también acciones de restitución en aquellos casos donde se hayan lesionado derechos de niñas, niños y adolescentes.

Se los suele llamar "nativos digitales"; sus vidas se desarrollan a través de las nuevas tecnologías, y a través de estas acceden a información, se divierten, aprenden y se relacionan. Del mismo modo están expuestos a mayores riesgos. La violación de la privacidad, la ciberviolencia, el ciberacoso, el *grooming*, encuentran en Internet un fructífero camino para desarrollarse.

Es obligación del Estado generar políticas públicas que garanticen a niñas, niños y adolescentes una "ciudadanía digital"[26] segura y libre de posibles afectaciones a sus derechos. Para ello, es necesario un rol activo por parte de la totalidad de las instituciones, con especial énfasis en la familia y la escuela.

El uso de Internet en las aulas es de gran utilidad en los procesos de enseñanza y aprendizaje, pero, por otro lado, también encierra un riesgo para niñas, niños y adolescentes que es fundamental tener presente a la hora de desempeñar el rol educativo. En este sentido es necesario que el docente genere espacios para reflexionar sobre el uso de las nuevas tecnologías. La comunidad educativa cumple un

26. Concebida como el ejercicio del derecho al acceso a las Tecnologías de Información y Comunicación (TIC) y a su apropiación, al desarrollo de habilidades digitales, al acceso a la información en línea de forma segura, transparente y privada, así como a la participación a través de medios tecnológicos. "Del uso seguro de Internet a la educación para la ciudadanía digital" en Tema Central del I Congreso Internacional Ciudadanía Digital - Edición 2010. Disponible en: http://www.congresociudadaniadigital.com/2010

rol preponderante en materia de prevención y protección ante los riesgos asociados al uso de los medios digitales, y debe promover conductas que refuercen el autocuidado de las alumnas y los alumnos, reconociendo su autonomía y capacidad para identificar situaciones riesgosas. Se requiere desarrollar acciones que promuevan el uso seguro de los medios digitales.

Desde el Ministerio Público Tutelar hemos llevado a cabo talleres con la comunidad educativa a fin de concientizar sobre las diferentes modalidades de violencia a la que están expuestos niñas, niños y adolescentes a través del uso de las nuevas tecnologías. Es de suma importancia intercambiar saberes y experiencias para comprender sus inquietudes y miradas en un mundo atravesado por la tecnología. Entendemos que esta es una forma de trabajo corresponsable, con un actor socializador fundamental como es la escuela en la vida de las niñas y los niños. Solo así se genera una comunidad alerta que resguarde y proteja derechos.

La mayoría de los adultos conoce mucho menos de Internet que sus propios hijos. La brecha digital suele ser muy amplia. Los cambios constantes e innovadores en relación con Internet generan desconocimiento continuo: cuando los adultos aprenden a utilizar una plataforma digital, surge otra que rápidamente es adoptada por niñas, niños y adolescentes, en un intento constante de alejarse de todo aquello que sea conocido y usado por el mundo adulto.

Los padres tienen la obligación indelegable de hablar con sus hijos respecto de los peligros que conlleva el uso masivo de las nuevas tecnologías, generar controles parentales conforme a la edad y autonomía de niñas, niños y adolescentes, sin invadir su privacidad, y estar alerta a los nuevos peligros a los que están expuestos sus hijas/os.

Para finalizar, debemos reflexionar en torno a la dualidad en el ejercicio de la protección: por un lado los progenitores ponderan los cuidados en relación con los niños y niñas, evitan la exposición en lugares públicos, el contacto y la interacción con extraños; sin embargo, esto se diluye cuando utilizan Internet y hacen uso de las nuevas tecnologías: los adultos relajan los cuidados cuando los niños y niñas están inmersos en sus computadoras, celulares u otros dispositivos móviles, y estos quedan expuestos al contacto e interacción con extraños.

Niñas, niños y adolescentes víctimas de delitos asociados al uso de las nuevas tecnologías

A pesar de los avances legislativos internacionales y nacionales, al detenernos en la relación existente entre la acción punitiva estatal y los derechos de niñas, niños y adolescentes con especial énfasis en su condición de víctimas, podemos observar el desvalor de la protección de las personas menores de edad, frente a los otros delitos (y/o sus correspondientes agravantes) que no los tienen por víctimas.

Haciendo un recorrido por las escalas penales del Código Penal Argentino podremos observar que, pese a que niñas, niños y adolescentes poseen un plus de derechos respecto del resto de la población debido a su condición de vulnerabilidad *per se*, por su condición de sujeto en formación, los delitos que los tienen por víctimas suelen detentar penas mucho más bajas que delitos cuyo bien jurídico tutelado es otro.[27]

Los Estados tienen la obligación convencional de adoptar medidas de protección que aseguren los derechos de niñas, niños y adolescentes durante los diversos procesos que los afectan –administrativos o judiciales–, especialmente en aquellos que los tengan como víctimas de violencia.

Al respecto, los estándares internacionales en materia de protección de derechos de niñas, niños y adolescentes víctimas de delitos conforman un fuerte *corpus juri internacional* que intiman a los Estados a brindar un plus de protección de derechos a esta franja etaria.

La CIDN contiene numerosos artículos que garantizan derechos instrumentales de niñas, niños y adolescentes inmersos en procesos judiciales que obligan a los Estados a garantizar la intimidad, la integridad física y psíquica, el derecho a ser oído y a contar con asistencia letrada especializada, entre otros. Entre sus invaluables aportes, el Comité

27. Ejemplo de ello es la escala penal del delito de abigeato contemplado en el Artículo 167 *ter* CP: "Será reprimido con prisión de DOS (2) a SEIS (6) años el que se apoderare ilegítimamente de UNA (1) o más cabezas de ganado mayor o menor, total o parcialmente ajeno, que se encontrare en establecimientos rurales o, en ocasión de su transporte, desde el momento de su carga hasta el de su destino o entrega, incluyendo las escalas que se realicen durante el trayecto. La pena será de TRES (3) a OCHO (8) años de prisión si el abigeato fuere de CINCO (5) o más cabezas de ganado mayor o menor y se utilizare un medio motorizado para su transporte". (Y los agravantes del artículo 167 *quater*.)

de los Derechos del Niño estableció que el derecho a ser oído y el interés superior son principios básicos que deben complementarse, ya que no es posible garantizar el interés superior del niño, si no se realizan todas las medidas necesarias para garantizar su derecho a ser oído.

Las Reglas de Brasilia sobre Acceso a la Justicia de las Personas en Condición de Vulnerabilidad definen a las personas en condición de vulnerabilidad como aquellas "que por su razón de edad, género, estado físico o mental, o por circunstancias sociales, económicas, étnicas y/o culturales, encuentran especiales dificultades para ejercitar con plenitud ante el sistema de justicia los derechos reconocidos por el ordenamiento jurídico", y agregan que causas de vulnerabilidad las constituyen "la edad, la discapacidad, la pertenencia a comunidades indígenas o a minorías, la victimización, la migración y el desplazamiento interno, la pobreza, el género y la privación de libertad".

Las Guías de Santiago sobre Protección de Víctimas y Testigos establecen que niñas, niños y adolescentes son víctimas definidas por la más alta vulnerabilidad, la cual viene dada por su propia condición y específicamente sostienen que

> ... los procedimientos en los que estén implicados menores deben estar afectados por términos de celeridad para que el menor no tenga que soportar la pendencia y la tensión que ello supone, pudiéndose iniciar cuanto antes las actuaciones de reintegración personal y psicológica.

Con respecto al testimonio establecen que debe llevarse a cabo evitando el riesgo de victimización secundaria y que el mismo debe darse en el marco del principio de excepcionalidad, procurando que sea un mínimo de veces, con tendencia a una única declaración. Asimismo, debe "extremarse el cuidado para que la víctima no coincida con el agresor".

El derecho internacional de los derechos humanos de niñas, niños y adolescentes fue recepcionado por nuestro derecho sustancial[28] y el derecho formal de las diferentes jurisdicciones, especialmente en lo concerniente a los códigos adjetivos de la Ciudad Autónoma de Buenos Aires[29] que establecen un trato diferenciado a esta población.

En este aspecto, y con el objeto de responder a los compromisos asumidos por el Estado Argentino en materia de protección de derechos

28. Ley N° 26061.

29. Leyes N° 2303 y N° 2451.

de niñas, niños y adolescentes víctimas de delitos, desde el Ministerio Público Tutelar trabajamos en pos de mejorar el servicio de justicia que se les brinda, no solamente en relación con el acceso[30] sino también en lo concerniente a garantizar su derecho a ser oído en todos los procesos judiciales que los afecten.[31] Para ello, maximizamos nuestros esfuerzos en pos de que el testimonio de niñas, niños y adolescentes se efectivice en un espacio acondicionado a sus necesidades. La Sala de Entrevistas Especializada del Ministerio Público cuenta con equipos de última tecnología que permiten que la declaración de niñas, niños y adolescentes se lleve a cabo en un lugar acorde a lo estipulado por los estándares internacionales, para que puedan dar su testimonio por única vez, evitando de esa forma el riesgo de revictimización.

El acceso independiente y en un piso diferenciado a la Sala de Observación permite que la niña, niño y/o adolescente no tome contacto con el agresor, ingresando por un sector especial, diferenciado del resto y sea recibido por psicólogos especialistas en infancia y adolescencia, en una sala especialmente acondicionada. El sistema de circuito cerrado de televisación y seguimiento remoto, con sistema integrado de grabación de audio y video, y de monitoreo de cada una de las cámaras en directo, posibilitan un registro fiel de la entrevista, a fin de que el testimonio cumpla con las formalidades de los actos únicos e irreproducibles.

Los delitos contra la integridad sexual de niñas, niños y adolescentes cuyo medio comisivo son las nuevas tecnologías avanzan de forma alarmante, y a su vez, el número de usuarios, y por lo tanto de posibles víctimas, aumenta notablemente.

En Argentina ocho de cada diez adolescentes usan Internet.[32] Interactúan de forma más predominante en las redes y plataformas digitales que en la vida real. Las niñas, niños y adolescentes se divierten, expresan, comunican, aprenden y se vinculan por Internet. Asimismo,

30. Oficinas de Atención Descentralizadas. Disponible en: http://www.mptutelar.gob.ar/oficinas-de-atencion y oficinas móviles. Línea de acceso WhatsApp: 15 70377037. Línea gratuita: 0800-122-7376. Asesoría Responde. Disponible en: http://www.mptutelar.gob.ar/asesoria-responde

31. Resolución AGT N° 71/2018, Sala de Entrevistas Especializada.

32. Encuesta Nacional sobre Acceso y Uso de Tecnologías de la Información y la Comunicación, INDEC. Disponible en: https://www.indec.gov.ar/uploads/informesdeprensa/entic_10_15.pdf

se vislumbra un descenso en las edades de las niñas y los niños que acceden por primera vez a las nuevas tecnologías, registrándose como edad promedio 10,8 años,[33] y evidenciándose un descenso en las edades de niñas y niños de nivel socioeconómico alto, quienes acceden en promedio a partir de los siete años.

Del estudio de casos realizado por *UNICEF* y *Global Kids Online*[34] surge que el lugar que prefieren los adolescentes para conectarse es su habitación, y que ocho de cada diez experimentaron una situación negativa con relación a su uso (exposición a cosas obscenas/pornográficas, violencia entre pares, maltrato, *bullying*, etc.). En cuanto a los encuentros con extraños, el 38 % de los encuestados manifestó haberse encontrado físicamente con alguien que conoció por Internet.

Debemos estar atentos a la dimensión del problema: el 80 % de los más de trece millones de adolescentes que viven en Argentina están expuestos a los peligros que conlleva el uso inadecuado de Internet.

Cuando una niña, niño o adolescente se encuentra inmerso en un proceso judicial que lo tiene como víctima del delito de *grooming* debemos redoblar los esfuerzos de todos los actores judiciales intervinientes a fin de que se pueda restituir el derecho vulnerado con la mayor celeridad posible, evitando la revictimización que genera *per se* el contacto con el sistema judicial.

Conclusiones

Estamos transitando una edad histórica presidida por las nuevas tecnologías, que repercuten en toda la sociedad y de manera especial en las niñas, niños y adolescentes, ya que alguna limitación en su acceso implicaría permanecer "excluido" de las relaciones entre pares. La edad promedio de inicio en las nuevas tecnologías es cada vez más baja, mientras que el uso y el acceso a las mismas tiende a su universalización. Esta situación interpela a los adultos a involucrarse en las nuevas tecno-

33. UNICEF, Kids Online Argentina, *Chicos Conectados. Investigación sobre percepciones y hábitos de niños, niñas y adolescentes en Internet y redes sociales*. Disponible en: https://www.unicef.org.ar/kidsonline/

34. Proyecto de investigación que busca fortalecer el conocimiento sobre el acceso, las oportunidades, los riesgos y la seguridad de niños, niñas y adolescentes en relación con los medios sociales e Internet. Ver: globalkidsonline.net

logías y en el uso de ellas; como así también a transitar junto a las niñas, niños y adolescentes el sendero de los avances tecnológicos.

Ahora bien, debemos reconocer que esos avances y usos no se condicen con la implicancia que se espera de los adultos en relación con los cuidados que se deben realizar para que niñas, niños y adolescentes estén ajenos a los peligros que conlleva el uso de Internet y, especialmente, de las redes sociales. Desde hace mucho tiempo, somos espectadores de una involuntaria incisión entre los mundos del adulto/tecnología e infancia/tecnología.

Por un lado, se reconoce la importancia de que la población acceda a las diferentes modalidades e instrumentos que brinda el servicio de Internet; pero a su vez, no se promueve suficientemente la necesaria implicación de las personas adultas para que, con una perspectiva de cuidado y protección, puedan acompañar apropiadamente a las niñas, niños y adolescentes en la exploración de un nuevo campo, que nos exige sostener una mirada permanentemente atenta.

Las garantías constitucionales reconocidas a las personas menores de edad nos obligan a indagar sobre aquellos compromisos que deben asumir el Estado y la sociedad en pos de generar un plus de protección de sus derechos; y esta protección extra no sólo debe darse en el ámbito punitivo, sino también a través de acciones de prevención, protección y restitución de los derechos vulnerados, en ámbitos tan diversos como el educativo, recreativo, cultural y familiar.

No alcanza solo con tipificar conductas delictivas, como el caso del *grooming*, sino que es necesario generar también políticas públicas de prevención, que otorguen información y herramientas a niñas, niños, adolescentes y adultos para generar una comunidad alerta, que pueda reflexionar y acompañar sobre el significado del derecho a la privacidad y de los peligros que entraña el uso inadecuado de las nuevas tecnologías.

Bibliografía

CILLERO BRUÑOL, Miguel, *Infancia, Autonomía y Derechos: una cuestión de principios*, Boletín del Instituto Interamericano del Niño, Nº 234.

COMISIÓN INTERAMERICANA DE DERECHOS HUMANOS, *Hacia la garantía efectiva de los derechos de niñas, niños y adolescentes: Sistemas Nacionales de Protección* (referencia: OEA/Ser. L/V/II.166), Doc. N° 206/2017.

CREUS, Carlos y BUOMPADRE, Jorge E., *Derecho penal. Parte especial*, Buenos Aires, Ed. Astrea, 7ª edición actualizada y ampliada, 2007.

Del uso seguro de internet a la educación para la ciudadanía digital, en Tema Central del I Congreso Internacional Ciudadanía Digital, Edición 2010. Disponible en: http://www.congresociudadaniadigital.com/2010

DONNA, Edgardo, *Delitos contra la integridad sexual*, Santa Fe, Ed. Rubinzal Culzoni, 2000.

GARIBALDI, Gustavo, "Aspectos dogmáticos del grooming legislado en Argentina", *Revista Derecho Penal*, año III, N° 7, mayo de 2014. Disponible en: http://www.saij.gob.ar

IGLESIAS, Susana; VILLAGRA, Helena y BARRIOS, Luis, "Un viaje a través de los espejos de los congresos panamericanos de niños", en *Del revés al derecho. La condición de la infancia en América Latina. Bases para una reforma legislativa*, Buenos Aires, Galerna/UNICEF/Unicri/Ilanud.

LERMA MORÓN, Esther, *Internet y Derecho Penal: hacking y otras conductas ilícitas en la red*, Navarra, Aranzadi, 2da ed., 2002.

UNICEF, *Chicos Conectados. Investigación sobre percepciones y hábitos de niños, niñas y adolescentes en internet y redes sociales*, Kids Online Argentina. Disponible en: https://www.unicef.org.ar/kidsonline/

UNODC, *Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children*, Viena, 2015. Disponible en: https://www.unodc.org/documents/commissions/CCPCJ/CCPCJ_Sessions/CCPCJ_23/E-CN15-2014-CRP1_E.pdf

VANINETTI, Hugo, "Inclusión del *grooming* en el Código Penal", *La Ley 2013-F-1200*, 2013.

VIANNA, Tulio, *Fundamentos de Direito Penal Informático*, Río de Janeiro, Editora Forense Jurídica, 2003.

Ciberdelitos. Desafíos para trabajar

Daniela Dupuy*

Introducción

Hoy la dinámica del cibercrimen y su evolución ha generado que delincuentes que hasta hace poco actuaban de manera aislada, sin coordinación y con un alcance local, ahora constituyan o formen parte de organizaciones transnacionales de ciberdelincuencia.

La profesionalización de delincuentes que perpetran delitos a través de Internet debido a la sofisticación de las técnicas utilizadas y a la disponibilidad de modernas herramientas, convierte en vulnerable a la sociedad –en aspectos de privacidad, intimidad, integridad sexual, honor, patrimonio, etcétera–, lo cual exige una nueva cultura y educación de los ciudadanos, con el objetivo de prevenir dichos ataques.

¿Qué facilita este escenario?

El fácil acceso al mercado ilegal de la tecnología, la dificultad de rastreo de actividades ilícitas en la *darknet*, las transacciones en moneda virtual, el mercado ilegal de datos, la débil armonización de la persecución penal internacional, etcétera.

Todo ello plantea nuevos desafíos en materia de seguridad digital que obligan a implementar estrategias que hagan frente a los requerimientos nacionales e internacionales.

La Convención de Budapest, firmada en 2001, y a la que la República Argentina adhirió en marzo de 2018,[1] es un instrumento fundamental que sirve como referencia para que todos los países que forman parte adapten sus legislaciones de fondo y de forma a las nuevas tecnologías, para que profundicen los mecanismos de Cooperación Internacional, toda vez que, es probable, atento a la transnacionalidad de estas modalidades delictivas, el autor se encuentre en un país, la

* Doctora en Derecho de la Universidad de Sevilla, España. Fiscal Penal a cargo del Equipo especializado en Delitos Informáticos de la Ciudad Autónoma de Buenos Aires.

1. Disponible en: www.coe.int

víctima en otro, y los datos necesarios para proceder, alojados en un servidor en otro país. Ello requiere armonización y coordinación internacional entre los países a fin de lograr investigaciones eficientes.

El objetivo de este trabajo es presentar brevemente los aspectos de derecho de fondo, las cuestiones procesales que se debería tener en cuenta en las investigaciones de entornos digitales y la preocupación e incertidumbre que hoy generan los algoritmos de inteligencia artificial, cuya aplicación en las investigaciones proporciona evidencia necesaria para comprobar un hecho delictivo.

Aspectos de derecho de fondo

Si bien hoy Argentina tiene una ley de Delitos Informáticos –Ley N° 26388–, considero que ella no conforma un catálogo cerrado de delitos pues, para la investigación de cualquier conducta delictiva, se necesita acudir, indefectiblemente, a la evidencia digital. Así, existen conductas que afectan directamente a sistemas informáticos –daño informático–; otras que utilizan los medios informáticos para su consumación –pornografía infantil– y tantas otras que durante su investigación penal se requiere acudir a evidencia digital. En este sentido, en un caso de homicidio, por ejemplo, seguramente una de las primeras medidas a adoptar será conocer la última conexión de la víctima y del victimario a Facebook o Instagram, y también los últimos ingresos a los buscadores de Internet.

La aparición de nuevas modalidades delictivas en entornos digitales nos obliga a evaluar si todas ellas deben ser alcanzadas por el derecho penal como instrumento adecuado para tutelarlas. Dicha pregunta exige analizar exhaustivamente cada conducta en particular a fin de diferenciar cuáles podrán tipificarse autónomamente en la legislación de fondo, o adecuarse a los tipos penales ya existentes; o bien, seleccionar las conductas que representan el ejercicio de determinados derechos individuales, ajenos a la intervención del Estado, y determinar si otras ramas del derecho –administrativo, civil, etc.– podrán asumir su tratamiento.

En este sentido, la ya conocida discusión en el ámbito del derecho penal se centra en el fenómeno expansionista, en confrontación con la estricta observancia del *principio de ultima ratio* e intervención mínima.

Sin adentrarnos en las ventajas y desventajas de ambos fenómenos a la luz de los avances tecnológicos, considero que ambos sistemas no solo no son incompatibles sino que se complementan.

En consecuencia, el derecho penal debe tutelar y equilibrar razonablemente las libertades individuales de los ciudadanos y la seguridad de la sociedad moderna ante los nuevos riesgos; pues no puede permanecer inmóvil ante los cambios sociales y los avances tecnológicos.

Algunas de las modalidades delictivas con las que nos enfrentamos a diario son las que siguen, y vale conocer básicamente en qué consisten y cómo se pueden prevenir.

Ataques de *malware*

Es la utilización del *software* para explotar vulnerabilidades en los sistemas. Un ejemplo de estos ataques es el *ramsonware*.

Es un *software* malicioso que permite bloquear y encriptar archivos de un sistema informático, y es frecuente que se solicite dinero –generalmente en *bitcoins* u otra criptomoneda y que sea depositado en una billetera virtual pues garantiza el anonimato del autor–, a cambio de quitar esa restricción.

Puede aparecer como adjunto o un *link* en un *e-mail* y cuando lo abrimos leeremos en nuestra computadora: "si deseas recuperar los archivos deberás depositar una cantidad determinada de *bitcoins* en una billetera virtual". El objetivo es que los sospechosos no puedan ser rastreados y permanezcan en el anonimato.

El *ramsonware* Wanna Cry, que significa "quiero encriptar", "quiero llorar", "quiero cifrar", atacó 230.000 sistemas en 150 países.

Encriptar o cifrar significa convertir un archivo en un amasijo incomprensible de *bits*.

Wanna Cry se creó sobre la base de una herramienta robada a la NSA llamada Eternal Blue que explota vulnerabilidades de Windows, y Microsoft, fabricante del sistema operativo de Windows, ya había alertado sobre esta vulnerabilidad.

Para prevenir que estos *malware* afecten nuestras computadoras, se debe invertir en mayor seguridad, actualizar el sistema operativo y activar el antivirus que lo detecta, no abrir archivos dudosos, etcétera.

Algunos sostienen que no se deben pagar las cifras que piden los cibercriminales a fin de desalentar la modalidad delictiva, pero lo cierto es que cuando el *malware* ataca a una empresa, entidad bancaria u organismo gubernamental, estos necesitan los datos que contienen los sistemas informáticos para poder funcionar, y entonces acceden a efectuar inmediatamente el pago.

Imaginemos que estos ataques de denegación de servicio no van dirigidos a particulares o a empresas sino a infraestructuras críticas; por ejemplo, una torre de control de un aeropuerto.

En este sentido es fundamental que gobiernos y empresas incluyan en sus agendas la aplicación de estrategias para proteger y garantizar la seguridad de sus infraestructuras críticas.

Fraudes

Son mecanismos utilizados por los defraudadores para que, a través del engaño provocado a las víctimas, obtengan de ellas toda la información necesaria sobre sus claves, datos sensibles, *e-mail* e información privada de los usuarios.

Esta información puede ser captada, a modo de ejemplo, cuando las mismas víctimas introducen sus claves en la página *web* de su entidad bancaria en la creencia que a ella pertenece, pero en realidad, es una página *web* clonada que presenta características casi idénticas a la original, que generan confusión en el usuario, quien introduce toda la información personal que es captada por el defraudador –*pharming*–.

Una vez que el defraudador se hizo de los datos sensibles de las víctimas pueden ocurrir dos cosas: a) que los venda, o b) que los utilice para realizar transferencias bancarias desde las cuentas de las víctimas en beneficio propio.

Para llevar a cabo la conducta b) es muy común que entre en juego una figura que cumple un rol específico: *el mulero*.

El *mulero* es una persona contratada por el defraudador y, a cambio de altas comisiones, procede a abrir una cuenta corriente a su nombre a la que el autor principal pueda transferir el dinero desde la cuenta ajena. Así, al recibirlo, el *mulero* sólo debe extraerlo y enviarlo vía Western Union, por ejemplo, a otro país, sin dejar rastros, en beneficio de quien posee el dominio del hecho.

Una dificultad que puede surgir de esta modalidad es la de determinar el grado de autoría o participación del *mulero*; pues muchas veces desconocen para qué deben abrir esa cuenta bancaria y el origen ilícito del dinero; aunque en otras ocasiones son parte de la misma organización criminal.

Es importante destacar que, cuando hablamos de delitos ciberecónomicos, es común que la criptomoneda sea utilizada por los cibercriminales para recibir el pago de sus víctimas sin posibilidad de ser rastreados.

La particularidad que tienen las criptomonedas, además de que hoy hay más de 800 tipos, es que no son emitidas por ningún banco.

Todas las transferencias de moneda virtual desde una a otra billetera virtual quedan registradas y cifradas para proteger la privacidad y seguridad de las transacciones en un enorme libro de cuentas llamado *blockchain*.

Blockchain es una gran base de datos segura por el cifrado, en la que debe haber varios usuarios que se encarguen de verificar y validar esas transacciones, y así el bloque correspondiente a esa transacción se registrará en ese libro de cuentas.

Pornografía infantil

Recientemente el Congreso ha sancionado la Ley N° 27436 que ha modificado el artículo 128 del Código Penal, aumentando la escala penal de 3 años a 6 años a quien

> … produjere, financiare, ofreciese, comerciare, publicare, facilitare, divulgare o distribuyere, por cualquier medio, toda representación de un menor de 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 meses a un año el que a sabiendas tuviere en su poder representaciones de las descriptas en el párrafo anterior.
>
> Será reprimido con prisión de seis meses a dos años el que tuviere en su poder representaciones de las descriptas en el primer párrafo con fines inequívocos de distribución, comercialización.
>
> Será reprimido con prisión de un mes a tres años el que facilitare el acceso a espectáculos pornográficos o suministrare material pornográfico a menores de 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 13 años.

La Fiscalía General de la Ciudad Autónoma de Buenos Aires firmó un Convenio con el National Center for Missing and Exploited Children (NCMEC) el día 11 de octubre de 2013.[2]

El NCMEC es una organización sin fines de lucro con sede en los Estados Unidos de América. Esta institución ha recibido apoyo del Congreso de los EE. UU. con el fin de construir una respuesta internacional coordinada e intercambiar información respecto de la problemática de los niños desaparecidos y explotados sexualmente.

Asimismo, el NCMEC ha obtenido autorización para establecer la *CyberTipline*, la cual proporciona un mecanismo centralizado donde los proveedores de servicios de Internet reportan actividades sospechosas relacionadas con la explotación sexual de los niños.

Así, a partir de la celebración del Convenio, el Ministerio Público Fiscal de la CABA tiene acceso a todos los reportes de actividades sospechosas que se detecten de usuarios de Internet en nuestro país.

Un dato significativo que demuestra la gravedad de la problemática de la distribución, difusión y tenencia de material de pornografía infantil es el creciente ingreso de casos.

Durante el año 2016 ingresaron 8823 reportes; en 2017, 23.086; y en el transcurso de 2018, 32.429; y efectuando una progresión para fin de año se espera un ingreso de más de 52.000 casos.

De este universo de casos que ingresan, se efectúa una selección temprana y algunos de ellos son archivados por diferentes motivos: atipicidad, carencia probatoria, oportunidad, nateos, etcétera.

El resto ingresa a la fiscalía para su correspondiente investigación y se suelen dar distintas situaciones en el marco del análisis de dispositivos de almacenamiento informático:

1. el sospechoso tiene cantidad de imágenes y videos de pornografía infantil;
2. el sospechoso tiene cantidad de imágenes y videos de pornografía infantil, y además las distribuyó o facilitó;
3. el sospechoso tiene cantidad de imágenes y videos de pornografía infantil, y además las distribuyó o facilitó, y también se de-

2. Resolución FG. 435/2013 de fecha 12/11/2013.

tectaron conversaciones –a través de medios informáticos– de contenido erótico o sexual, entre el mayor y un menor de edad;

4. el sospechoso tiene cantidad de imágenes y videos de pornografía infantil, y además las distribuyó o facilitó, y también se detectaron conversaciones –a través de medios informáticos– de contenido erótico o sexual, entre él y un menor de edad, y además hay prueba –digital y/o física– de abuso sexual y/o corrupción de menores.

Ante cualquiera de estos posibles escenarios, y frente a la posibilidad de efectuar un análisis interconectándolos, se desprende una clara conclusión, internacionalmente aceptada:

Quien consume o *tiene* imágenes o videos de pornografía infantil no se conforma con unos pocos, cada vez quiere más y diferentes, para proceder a su prolija clasificación en edades de los niños, sexo y acto sexual que realiza. Dicha *demanda* genera la necesidad de mayor *oferta*; situación que conlleva a tener que *producir* más material para satisfacer los pedidos; y esa producción se traduce en la consumación de *abuso sexual de menores*.

Pero a su vez, el que demanda y recibe debe dar algo a cambio: más material y diferente; debe *distribuir*, *facilitar*.

Conclusión: no es posible *tener* material de pornografía infantil sin que antes alguien haya *abusado sexualmente de un niño*.

Así lo explica Fernández Teruelo cuando expresa que dicho criterio se fundamenta en que

> … tanto los actos de difusión de pornografía infantil como los relacionados con la misma pueden determinar –con base en la experiencia general– un aumento de la oferta. De este modo, la puesta en el mercado de estos materiales generaría nuevas necesidades estimulando la demanda. Si aumenta la demanda aumentará también la oferta, y la oferta solo puede satisfacerse utilizando a menores de carne y hueso en prácticas de naturaleza sexual para tomar las imágenes o realizar grabaciones en otros soportes.[3]

Entonces, esta es la razón que justifica la intervención penal; y no el hecho de obtener satisfacción sexual con la contemplación de imágenes de menores, lo que en realidad queda dentro de la moral sexual de cada uno.

3. Fernández Teruelo, Javier G., en Dupuy, Daniela (dir.), *Cibercrimen. Aspecto de Derecho Penal y Procesal Penal*, Madrid, BdeF, 2016, p. 63.

En consecuencia, el fundamento para castigar a la persona que consume material pornográfico con menores de edad se basa en que la demanda incide directamente en el aumento de oferta, y para ello será necesario producir aún más cantidad de material pornográfico con la intervención de menores, vulnerando permanentemente su integridad sexual y el libre desarrollo de la sexualidad.

Grooming

La captación de niños en línea es el proceso por el cual un mayor de edad, por medio de Internet, trata de ganarse la amistad de un menor de edad con fines sexuales; en ocasiones a través de conversaciones eróticas, en otras mediante *webcam*, solicitándole fotos o videos del menor con contenido sexual, pudiendo utilizar el autor estas imágenes ya sea para satisfacer sus necesidades libidinosas o bien para introducirlas en una red internacional de pornografía infantil.

El acecho al menor suele ser paulatino, con un nivel de seducción tal que aquel no alcanza a advertir la gravedad, pero cuando la advierte y quiere retirarse del "juego", suele ser amenazado o extorsionado para que no lo haga.

Nuestro Código Penal ha receptado esta modalidad delictiva en el artículo 131, susceptible de la necesidad de ajustar o modificar el tipo penal a fin de poder subsumir eficientemente cada proposición fáctica –hecho– a cada uno de los elementos normativos del delito.

> Será penado con prisión de seis meses a cuatro años el que, por medio de comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos, contactare a una persona menor de edad, con el propósito de cometer cualquier delito contra la integridad sexual de la misma.

Son varias las críticas que pueden hacerse a este tipo penal: una pena alta equiparada al abuso sexual simple; la no especificación de que el autor debe ser un mayor de edad; la falta de coherencia con la sistémica del Código Penal en cuanto al menor de 13 años y, entre 13 y 16 años cuando mediare engaño, abuso de autoridad o intimidación.

La cantidad de denuncias que ingresan al sistema se acrecientan incesantemente, por lo que entiendo que es fundamental la presencia de fuertes políticas de Estado tendientes a prevenir la comisión de es-

tas conductas, a través del suministro de información sobre las consecuencias del *grooming* y del uso no cuidado de las redes sociales.

Los destinatarios del mensaje formativo que tiende a prevenir la comisión de este delito debe dirigirse a niños –por lo general las víctimas son entre 8 y 13 años–, a sus padres y a los docentes.

Revenge porn

Se suele llamar así a la difusión –no consentida– de imágenes y videos de contenido generalmente sexual o erótico, captadas con el asentimiento de la víctima, en un lugar privado, fuera del alcance de la mirada de terceros.

Por lo general, estas modalidades se llevan a cabo cuando quien tiene en su poder el material sexual, ya sea por haber sido captado por él mismo, o porque lo recibió de un tercero, lo publica o difunde sin tener en cuenta la vulneración a la privacidad o intimidad de la víctima que, si bien prestó conformidad para que se ejecute la captación u obtención de imágenes o grabaciones audiovisuales, no lo hizo con respecto a su posterior difusión.

Dicha conducta suele causar un daño irreversible en la damnificada pues lo que se difunde, cede o revela es muy difícil quitarlo de la órbita virtual y las consecuencias perduran en el tiempo.

Aunque no siempre, es muy común que estas modalidades se cometan en razón de una ruptura de pareja y en venganza –de allí su nombre– se publican las imágenes íntimas.

También es habitual que la difusión conforme un eslabón más de la cadena de violencia contra la mujer en el ámbito de una pareja, circunstancia que se agrega al control de los contactos de la víctima, de sus movimientos, sus amistades, sus contraseñas, y a la difusión de imágenes y videos íntimos.

En la Argentina aún no es delito y considero que un buen ejemplo a seguir es la legislación penal española.[4]

4. Art. 197.7 LE: "Será castigado con una pena de prisión de tres meses a un año o multa de seis a doce meses el que, sin autorización de la persona afectada, difunda, revele o ceda a terceros imágenes o grabaciones audiovisuales de aquella que hubiera obtenido con su anuencia en un domicilio o en cualquier otro lugar fuera del alcance de la mirada de terceros, cuando la divulgación menoscabe gravemente la intimidad personal de esa persona. *La pena se impondrá en su mitad superior cuando los hechos hubieran sido*

Ahora bien, el 7 de enero de 2019 la Legislatura introdujo una modificación a la Ley Contravencional N° 1472, a través de la cual se incorpora el Capítulo V, denominado Identidad digital de las personas, que en su artículo 71 *bis* se refiere concretamente a la *Difusión no autorizada de imágenes o grabaciones íntimas y señala*:

> Quien difunda, publique, distribuya, facilite, ceda y/o entregue a terceros imágenes, grabaciones y/o filmaciones de carácter íntimo sin el consentimiento de la persona y a través de cualquier tipo de comunicación electrónica, de transmisión de datos, página *web* y/o a través de cualquier otro medio de comunicación, siempre que el hecho no constituya delito, es sancionado con una multa de cuatrocientas (400) a mil novecientas cincuenta (1950) unidades fijas, o cinco (5) a quince (15) días de trabajo de utilidad pública o con tres (3) a diez (10) días de arresto. El consentimiento de la víctima para su difusión, siendo menor de 18 años, no será considerado válido. Tampoco podrá alegarse el consentimiento de la víctima en la generación del contenido como defensa a la realización de la presente conducta.[5]

El problema de esta nueva normativa es que, al ser una contravención, las sanciones son considerablemente bajas en relación a si dicho comportamiento fuera un delito. También es de destacar que la contravención es de alcance estrictamente local, es decir, deberá cometerse dentro de la órbita de la Ciudad Autónoma de Buenos Aires pues la Ley N° 1472 tiene sus efectos únicamente en dicha ciudad.

El *sexting* es una modalidad parecida a la recientemente mencionada, pero se lleva a cabo entre jóvenes y adolescentes.

Ellos han naturalizado compartir y difundir videos y fotografías eróticas y sexuales, pero sin medir las consecuencias.

Su difusión permitiría que cualquier abusador que se encuentra al acecho en las redes pueda captar esas imágenes y utilizarlas para extorsionar o amenazar al menor de edad, para que le envíe otras fotos o videos de la misma naturaleza, o bien, introducir aquellas en una red internacional de pornografía infantil, con sus graves implicancias.

---

cometidos por el cónyuge o por persona que esté o haya estado unida a él por análoga relación de afectividad, aun sin convivencia, la víctima fuera menor de edad o una persona con discapacidad necesitada de especial protección, o los hechos se hubieran cometido con una finalidad lucrativa".

5. Art. 71 *ter*. "Difusión no autorizada de imágenes y grabaciones íntimas", Capítulo V, Identidad Digital de las personas, Ley N° 6128/2019, modificatoria de la Ley N° 1472, 7/02/2019.

El *sexting* no es delito en la Argentina, y entiendo que no debería serlo. El hecho de que los autores suelen ser menores de edad alcanza para abordar la problemática fuertemente desde la educación, formación y prevención.

Aspectos procesales

Habiendo efectuado una somera descripción de las nuevas modalidades delictivas que se realizan en entornos digitales, es necesario resaltar la importancia que implica la presencia de normas procesales adaptadas a las nuevas tecnologías para lograr investigaciones eficientes.

En este sentido, si bien es cierto que el principio de libertad probatoria permite utilizar normas procesales análogas para investigar, también lo es que abusar de aquel podría afectar las garantías constitucionales de los sospechosos.

Partimos de la base de que no es lo mismo secuestrar prueba física que evidencia digital.

La mayoría de los códigos procesales hacen referencia a objetos o cosas, pero no a datos. En la práctica, sin embargo, lo que se necesita incautar en las investigaciones en entornos digitales son los datos que se encuentran dentro de la cosa: el dispositivo de almacenamiento informático (PC, iPad, *pen drive*, *smartphone*, etc.).

Imaginemos, por ejemplo, un registro domiciliario para encontrar drogas. Seguramente, el personal policial registrará los lugares físicos posibles donde pueda hallarse la sustancia estupefaciente dentro de una finca determinada. Ahora bien, supongamos que esa búsqueda se dirige a encontrar imágenes de pornografía infantil en un teléfono o en una computadora. Allí, al requisar con autorización del juez, quizás encontremos lo que buscamos, pero también la vida de su titular; lo que guardó hace cinco años, datos provenientes de otro delito, o bien información de algún familiar que utiliza también ese dispositivo. Entonces la expectativa de privacidad es mucho menor en el segundo caso que en el primero. Ello merece una reflexión y debate.

Asimismo, los registros permitidos en las normas procesales se dirigen expresamente a lugares físicos: fincas, organismos, edificios públicos.

Pero cuando se registran datos informáticos puede ocurrir que:

a. Los datos no fueron almacenados en discos duros locales, sino en un servidor externo al cual se accedió por Internet;
b. Almacenamiento de datos en la nube;
c. Datos almacenados en un sistema informático en el extranjero;
d. Utilización de medios de comunicación anónimos: TOR o terminales públicas.

Entonces es muy importante que las órdenes de registro tengan cierta flexibilidad; si los operadores se encuentran ante cualquiera de las situaciones anteriores, deben poder extender el registro a ese sistema informático.

Es fundamental la posibilidad de extender rápidamente el registro o el acceso a otro sistema cuando haya motivos para creer que los datos buscados se encuentran en otro sistema informático, pues corremos el riesgo de que la información se pierda dada la volatilidad de los mismos.

Asimismo, las escuchas telefónicas fueron reemplazadas por el intercambio de datos vía *e-mail* o llamadas de voz por IP, y su intervención plantea dificultades, pues el éxito de este tipo de investigaciones depende de la capacidad de interceptar los datos de tráfico de las telecomunicaciones.[6]

Ello trae aparejadas algunas dificultades técnicas y jurídicas; pues no es lo mismo la autorización para grabar una conversación telefónica que interceptar los procesos de transferencia de datos.

Las cuestiones previamente señaladas frecuentemente generan objeciones acerca de la legalidad de la recolección de la evidencia digital, y ello amerita la discusión sobre la adaptación de las leyes procesales al avance tecnológico, tal como lo recoge la Convención de Budapest en sus artículos 16 a 20.[7]

Asimismo, la experiencia en investigaciones complejas me hacen reflexionar acerca de la necesidad de incorporar nuevas y modernas herramientas tecnológicas para comprobar el hecho que se investiga.

6. Es la información sobre el circuito de una comunicación realizada por medio de un sistema informático: origen, destino, ruta, hora, duración y fecha de la comunicación.

7. Muchos países que adhirieron a Budapest ajustaron sus códigos procesales a las nuevas tecnologías –España y Portugal son un excelente ejemplo de ello–. Aunque en la República Argentina, la provincia del Neuquén ha modernizado su Código Procesal contemplando las diferentes situaciones esbozadas.

En consecuencia, la incorporación de las figuras del agente encubierto, agente revelador, informante, como así también los diferentes tipos de vigilancia –acústica y remota sobre equipos informáticos a través de dispositivos de seguimiento de localización– potenciarían la capacidad de investigación y otorgarían tecnología de avanzada para lograr resultados eficientes en el marco de la investigación penal. Claro que siempre con los recaudos necesarios para evitar vulnerar garantías constitucionales.

Inteligencia artificial y *big data*: robots en acción

No sé si nos damos cuenta de lo rápido que nos estamos precipitando hacia lo desconocido. Aunque algunos expertos comienzan a familiarizarse con los avances de la inteligencia artificial, la nanotecnología, la *big data*, creo que aún nadie es realmente experto en todos esos ámbitos, es decir, nada hoy puede aún conectar todos los puntos y ver la imagen entera; ni las mentes más brillantes son capaces de adivinar cómo podrían impactar los descubrimientos en inteligencia artificial en la tecnología y viceversa. Nadie puede absorber todos los descubrimientos científicos a la vez, procesar la infinita información que aquellas herramientas nos brindan con tanta precipitación y sin posibilidad de detener el sistema.

Esta es una de las razones por las que es muy importante pensar en la nueva agenda de la humanidad; porque tenemos la posibilidad de interiorizarnos con respecto al uso de las nuevas tecnologías, sería lógico que entendiéramos qué está sucediendo y decidiéramos qué hacer al respecto antes de que ellas decidan por nosotros.[8]

En esta línea, un interrogante es ¿cómo la justicia y la sociedad deberían manejar el uso de la inteligencia artificial aplicada a los robots en el contexto de la aplicación de la ley?[9]

8. Harari, Yuval N., *Homo Deus. Breve historia del mañana*, Buenos Aires, Ed. Penguin Random House, 2017, p. 69.

9. Reid, Melanie, "Rethinking the Fourth Amendment in the Age of Supercomputers, Artificial Intelligence, and Robots", *WVU Rev.* 863, Lexis Nexis, Vol. 119, N° 3, abril de 2017.

Es interesante y preocupante al mismo tiempo discutir acerca de cómo va a gestionar y validar el sistema judicial la evidencia adquirida por robots durante la prevención e investigación.

En esa línea, los robots ¿serán más inteligentes, rápidos y eficientes que los oficiales humanos? Una vez que la tecnología de inteligencia artificial se combina con un robot completamente humanoide capaz de caminar, correr, saltar y comunicarse con los humanos, podría ser una herramienta para hacer cumplir la ley. Ejemplo de ello, un robot con *GPS* podría obtener datos de geolocalización inmediatamente para identificar la ubicación física de un dispositivo electrónico; podría acceder a la cámara de vigilancia pública en tiempo real; podría usar *software* de imágenes, lectura de matrículas y reconocimiento facial para identificar posibles sospechosos; todo en cuestión de segundos o minutos, en lugar de días o semanas, y en comunicación directa con el fiscal que investiga.

Asimismo, la capacidad de estos programas de ejecutar una orden de registro será seguramente muy útil para la aplicación de la ley, pues se generará un registro digital completo de cuándo se obtiene una orden de búsqueda, qué evidencia se recopila, cómo se hará conocer al investigador los rastros digitales encontrados.

Claro que el ahorro de tiempo sería significativo: hoy debemos esperar días para que una empresa de telefonía celular responda a un requerimiento, y las herramientas de investigación que nos brindará la inteligencia artificial son muy superiores en comparación con las que hoy poseemos debido a los escasos y limitados recursos humanos y/o financieros.

En consecuencia, es probable que la aplicación de la ley tenga potencialmente la capacidad de resolver más crímenes e incluso prevenir delitos futuros a través del análisis predictivo.

Si bien las posibilidades mencionadas pueden animar la obtención de resultados eficientes en tiempos inmediatos, entiendo que debemos comenzar a discutir y a analizar su validez, su eventual intromisión exorbitante a la intimidad de las personas y vislumbrar su puesta en escena en un juicio oral público, cuando debamos explicar la metodología utilizada para obtener esa evidencia en tiempo récord.

No hay duda de que los robots diseñados a través de programas de inteligencia artificial interferirán en el derecho a la privacidad de los ciudadanos con mayor frecuencia que los oficiales humanos, toda

vez que tendrán acceso a mayor cantidad de datos de los sospechosos y de terceros en un período de tiempo más corto; pues la era de la información ha multiplicado exponencialmente la cantidad de datos personales producidos y recolectados anualmente.

Así, las herramientas de investigación de las fuerzas del orden han crecido en sofisticación y pueden realizar búsquedas mucho más intrusivas entre los papeles y efectos de los ciudadanos. La cantidad de datos capturados en Internet a diario es inimaginable, y los investigadores criminales pretenden aprovechar esos datos para conectar los puntos en una investigación, y para predecir y prevenir el crimen.

Como se resaltó más arriba, varios departamentos de policía y agencias federales de Estados Unidos ya están usando la tecnología para realizar predicciones y análisis de contenido y gestión de diferentes bases de datos. Ello desencadena constantes inquietudes en relación con la protección de la Cuarta Enmienda, toda vez que el acceso a una base de datos sin límites requiere un replanteamiento completo de la doctrina de la Cuarta Enmienda y analizar a conciencia tal intrusión para determinar si se requiere una orden judicial.[10]

En este sentido, el resultado obtenido de la utilización de las herramientas inteligentes que se traducirán muchas veces en evidencia en el marco de una investigación deberá ser analizado a la luz del principio de libertad probatoria.

Es indudable que los algoritmos aplicados a los robots exigirán supervisión e intervención humana cuando accedan a los datos.

En ese sentido, las búsquedas digitales representan una preocupación pues las fuerzas del orden público pueden abusar fácilmente de búsquedas abiertas, accediendo a una cantidad enorme de datos. Desde el pasado, el requisito de las garantías fue una solución; se identifica a un sospechoso, se recopilan pruebas y se obtiene una orden. Sin embargo, en las investigaciones en entornos digitales no habrá ningún sospechoso hasta después de que el análisis de los megadatos señale a un individuo en particular. Esta poderosa herramienta debe ser monitoreada de cerca, pero de una manera que no obstaculice la eficiencia y la recolección de la evidencia para el éxito de la investigación.

10. "United States v. Jones", 565 U.S. 400, 2012.

Históricamente, la regla de exclusión ha tenido un efecto disuasorio para estos casos.[11] Agentes de policía y del gobierno se mantuvieron bajo control por temor a una demanda si la persona equivocada era arrestada, y la necesidad de obtener una orden sirve como control de la acción policial general. Es decir, que la amenaza de una acción civil, sanciones penales, despidos o suspensiones laborales en casos de abusos flagrantes de poder contra un ciudadano inocente o su propiedad, pueden disuadir la mala conducta de agentes policiales y/o funcionarios humanos.

La pregunta es: ¿Estos mismos elementos de disuasión funcionarían en un robot creado por algoritmos de inteligencia artificial?

Y más, si los robots cometen violaciones constitucionales, los acusados en causas penales deberán presentar sus quejas ¿contra una máquina?, ¿contra el usuario?, ¿contra los diseñadores o ingenieros informáticos que la programaron?

Conclusiones

1. Es fundamental que los investigadores tengan un amplio conocimiento de las nuevas modalidades delictivas que se llevan a cabo en entornos digitales, así como del modo en que se investigan y de qué forma se resguarda, se analiza y se presenta la evidencia digital.
2. Este conocimiento alcanza a la investigación de cualquier tipo de delitos pues siempre va a ser necesario acudir a evidencia digital para su comprobación.
3. Son importantes las modificaciones legislativas necesarias cuando se advierten ciertas falencias –como en el *grooming*– o bien cuando la aparición de nuevos comportamientos amerite su inclusión en el Código Penal.
4. Adaptar los códigos procesales a los avances tecnológicos. No se pueden resolver los nuevos conflictos con las herramientas utilizadas en el siglo XX pues los problemas ahora son diferentes.
5. La intensa capacitación de jueces, fiscales y defensores y de sus equipos deviene vital a la hora de abordar esta problemática.

11. Heffernan, W. C., "The Fourth Amendment Exclusionary Rule as a Constitutional Remedy", 88 *Geo.L.J.* 799, 864, 2000.

6. Entra en juego un nuevo actor: el sector privado. La información inicial en una investigación es proveída por las empresas proveedoras de servicios de Internet. Si bien ellos no tienen regulada su obligatoriedad en responder a los requerimientos judiciales, lo cierto es que conocer los alcances de los requisitos a cumplir para hacerse de esa información acelera los tiempos.
7. Es necesario profundizar la Cooperación Internacional. La actuación aislada e independiente de los diferentes países resulta ineficaz. Es fundamental la armonización de los ordenamientos jurídicos de cada país y los criterios de persecución penal, para ofrecer soluciones legales ante las nuevas situaciones que surjan, lo cual debe hacerse armónicamente con la actividad de otros Estados y con las pautas y criterios asumidos internacionalmente.
8. El compromiso de trazar lineamientos de políticas públicas con una mirada responsable, proactiva y formativa para mitigar estos comportamientos.
9. El desafío es poder procesar esa gran cantidad de información en el marco de una investigación penal, captar y optimizar los resultados provenientes de un algoritmo de inteligencia artificial, y validar toda la prueba en un juicio oral bajo los estándares de absoluto respeto a las garantías constitucionales y derechos fundamentales como la intimidad y la privacidad de los ciudadanos, entre tantos otros derechos inherentes a los mismos.

Bibliografía

ABOSO, Gustavo Eduardo, *Derecho penal cibernético. La cibercriminalidad y el Derecho penal en la moderna sociedad de la información y la tecnología de la comunicación*, Buenos Aires, BdeF, 2017.

ACALE SÁNCHEZ, María, "Análisis del Código Penal en materia de violencia de género contra las mujeres desde una perspectiva transversal", en VILLACAMPA ESTIARTE, Carolina (coord.), *Violencia de género y sistema de justicia penal*, Valencia, Tirant Lo Blanch, 2008.

AGUSTINA SANLLEHÍ, José Ramón, "Cibercriminalidad y perspectiva victimológica: un enfoque general explicativo de la cibervictimización", en *Cuadernos de Política Criminal*, Nº 114, III, Época II, 2014.

_____, "Menores infractores o víctimas de pornografía infantil. Respuestas legales e hipótesis criminológicas ante el Sexting", Catalunya, en *Revista Electrónica de Ciencia penal y Criminología*, 2010.

ÁLVAREZ VIZCAYA, Maite, "Consideraciones político-criminales sobre la delincuencia informática: el papel del Derecho penal en la red", en *Cuadernos de Derecho Judicial*, Escuela Judicial, Consejo General del Poder Judicial, Internet y Derecho Penal, 2001.

BUOMPADRE, Jorge Eduardo, *Violencia de género en la era digital*, Buenos Aires, Ed. Astrea, 2016.

CORCOY BIDASOLO, Mirentxu, "Problemática de la persecución penal de los denominados delitos informáticos: particular referencia a la participación criminal y al espacio ámbito temporal de comisión de los hechos", Eguzkilore, *Cuaderno del Instituto Vasco de Criminología*, N° 21, 2007.

DAVIS, Frederick T., "A U.S. Prosecutor's Access to Data Stored Abroad - Are There Limits?", p. 4 y ss., en *The International Lawyer. A triannual publication of the Aba/Section of International Law*, Vol. 41. N° 1, 2015. Disponible en: https://www.americanbar.org/content/dam/aba/uncategorized/international_law/til_49-1_cpy.authcheckdam.pdf [fecha de consulta: 26 de agosto de 2018].

DUPUY, Daniela (dir.) y KIEFER, Mariana (coord.), *Cibercrimen, II, Nuevas conductas penales y contravencionales. Inteligencia artificial aplicada al Derecho penal y procesal penal. Novedosos medios probatorios para recolectar evidencia digital. Cooperación Internacional y Victimología*, Buenos Aires, Ed. BdeF, 2018.

FERNÁNDEZ TERUELO, Javier G., en DUPUY, Daniela (dir.), *Cibercrimen. Aspecto de Derecho Penal y Procesal Penal*, Madrid, BdeF, 2016.

HARARI, Yuval N., *Homo Deus. Breve historia del mañana*, Buenos Aires, Ed. Penguin Random House, 2017.

IANELLO, Romina y VELTANI Darío, "La pornovenganza en el Derecho penal argentino", en DUPUY, Daniela y KIEFER, Mariana (dirs.), *Cibercrimen II*, Buenos Aires, BdeF, 2018.

JIMÉNEZ DÍAZ, María José, "Sociedad del riesgo e intervención penal", en *Revista electrónica de Ciencia Penal y Criminología*, RECPC 16-8, 2014.

JIMÉNEZ MARTIN, Jorge, "Los delitos informáticos en el ámbito de la violencia de género: algunas reflexiones", en DUPUY, Daniela (dir.), *Cibercrimen, Aspectos de Derecho penal y procesal penal. Cooperación Internacional. Recolección de evidencia digital. Responsabilidad de los proveedores de servicios de Internet*, IPS, Buenos Aires, Editorial BdeF, 2016.

KERR, Orin, *Computer Crime Law. Fourth Edition*, American Casebook Series, West Academic Publishing, 2018.

_____, "Summer 2018 Case Supplement", ed. West.

MIRÓ LLINARES, Fernando, *El cibercrimen. Fenomenología y Criminología de la delincuencia en el ciberespacio*, Madrid, Editorial Marcial Pons, 2012.

OBSERVATORIO DE LA SEGURIDAD DE LA INFORMACIÓN, *Guía sobre adolescencia y sexting ¿Qué es y cómo prevenirlo?*, Madrid, Instituto Nacional de Tecnologías de la Comunicación, 2011.

OLMEDO CARDENETE, Miguel, "¿Es la *lex stricta* una garantía efectiva en Derecho penal?", en GARCÍA VALDÉS (coord.) y otros, *Estudios penales en homenaje a Enrique Gimbernat*, vol. I, 2008.

PALAZZI, Pablo, "Difusión no autorizada de imágenes íntimas (revenge porn)", *El Derecho, Diario de Doctrina y Jurisprudencia*, Buenos Aires, 2016.

_____, "El delito de difusión no autorizada de imágenes íntimas", en DUPUY, Daniela (dir.), *Cibercrimen*, Ed. BdeF, 2016.

PÉREZ DE ACHA, Gisela (coord.), *Internet en México: Derechos humanos en el entorno digital*, México, Editorial de derechos digitales, 2016. Disponible en: https://creativecommons.org/licenses/by-sa/4.0/deed.es

SALT, Marcos, "La relación entre la persecución de delitos informáticos y el Derecho penal internacional", en *Informática y delito*, Buenos Aires, Editorial Infojus, 2014.

_____, *Nuevos desafíos de la evidencia digital: Acceso transfronterizo y técnicas de acceso remoto a datos informáticos*, Buenos Aires, Ad-Hoc, 2017.

SALVADORI, Iván, "La controvertida relevancia penal del *sexting* en el Derecho italiano y comparado", *Revista Electrónica de Ciencia Penal y Criminología*, 2017.

VARGAS DE BREA, Paula, *La regulación de la pornografía no consentida en Argentina*, Buenos Aires, Libertad de Expresión e Internet, CELE.

Internet y las nuevas formas sociales, jurídicas y punitivas

Alejandro Fernández*

Masificación de Internet y nuevas tecnologías

Internet está de moda. Según la Real Academia Española "estar de moda" es una expresión que nos permite señalar cuando un tipo de vestimenta, conducta o uso de algún producto u objeto se ha generalizado lo suficiente como para marcar tendencia y/o convertirse en vanguardia.

De acuerdo con *Global Digital Report in 2018 "We are social"*, hay en el mundo 4 billones de usuarios de Internet. Esto equivale a un nivel de penetración del 53%. En Argentina, el nivel de penetración alcanza el 78%, contabilizando usuarios residenciales y organizacionales, lo que equivale a casi 32 millones de usuarios. Internet, o más específicamente el uso de Internet, se ha generalizado. Sin dudas, entonces, la "www" está de moda, es vanguardia y marca tendencia.

Para la estadística, la moda es el valor que más se repite en una variable determinada. Internet es moda porque es el medio y el recurso privilegiado por la sociedad tanto para la búsqueda de información (uso tradicional) como para el establecimiento de relaciones sociales (nuevo uso).

* Actual Vicepresidente del Consejo de la Magistratura de la Ciudad Autónoma de Buenos Aires. Abogado, recibido en la UBA, Magíster en Comunicación Política y Gobernanza en la George Washington University y especialista en Administración y Derecho de la Seguridad Pública en la Escuela de Posgrado Ciudad Argentina, Universidad Carlos III de Madrid y Universidad del Salvador. Entre los numerosos cargos que desempeñó, se destacan haber sido Auditor General de la Ciudad Autónoma de Buenos Aires, Subsecretario de Asistencia Técnico Administrativo de la Legislatura porteña, Director General de Recursos Humanos del Ministerio del Interior e Interventor de la Dirección de Admisión de Extranjeros como así también Coordinador del Comité de Seguridad en el Fútbol perteneciente a la Secretaría de Seguridad Interior, del Ministerio del Interior.

En términos generales, las modas permiten a los hombres y mujeres participar y aprovecharse de un mecanismo de coordinación social. Los mecanismos de coordinación social sirven para establecer parámetros de relación entre los individuos, reglas fundamentales para la convivencia, sirven en la generación de representaciones colectivas de orden y ofrecen estrategias para anticipar desafíos futuros.

Si aceptamos la premisa que Internet está de moda y es moda entonces la red se ha transformado en un nuevo mecanismo de coordinación social que utiliza nuevos dispositivos, modifica las relaciones sociales y ofrece nuevos roles en la sociedad. La red como mecanismo de coordinación social combina la comunicación vertical –propia de la coordinación estadocéntrica– con la horizontal –característica de la coordinación vía mercado–. Las relaciones allí son más informales, no requieren de la formación de nuevas organizaciones.[1]

De ahí entonces que Manuel Castells[2] hable de "sociedad red".

En la *sociedad red* Internet ya no es un recurso exclusivo de investigadores, científicos y gobiernos, en especial del ala militar de los gobiernos. Internet ya no es un mero medio de comunicación que culmina con la revolución tecnológica iniciada con la radio en las postrimerías del siglo XIX. Internet no solo permite comunicarse más, mejor y más rápido, sino que además amplía formidablemente el espacio público.[3] La ampliación difumina el límite entre lo público y lo privado incorporando las conversaciones privadas en el espacio público. En especial a partir de la aparición de las así llamadas redes sociales.

Llama nuestra atención que se denomine redes sociales a Facebook, Instagram, Twitter, como si previo a Internet no existieran las redes sociales. La digresión sociológica sobre el apelativo excede el objetivo de este pequeño artículo aunque vale la pena dejar señalado el punto como muestra de los cambios más profundos, incluidos el lenguaje y las construcciones teóricas, que provoca Internet y que aún no advertimos o no hemos tenido el tiempo de analizar en profundidad.

1. Oaets, S., Owen, D., y Gibson, R. (eds.), *The Internet and politics. Citizens, voters and activists*, Nueva York, Routledge, 2006.

2. Castells, Manuel, *The Information Age. Economy, Society, and Culture*, Oxford, Wiley Blackwell, 2010.

3. Cardon, Dominique, *La democracia Internet. Promesas y límites*, Buenos Aires, Editorial Prometeo, 2010.

Internet ha venido atravesando un proceso creciente de masificación. La masificación no es solo tecnológica, de un aumento de los dispositivos; es fundamentalmente de uso. Internet pasa de ser un recurso para el uso científico a servir para usos domésticos, lúdicos, comerciales y prácticos. La masificación de esos usos constituye un cambio de escala y modifica la estructura social de la red. De ser una comunidad pequeña y homogénea social y culturalmente se transforma en un espacio que es ocupado por poblaciones cada vez más heterogéneas geográfica, social y culturalmente.[4]

La masificación es causa y resultado de la aparición de las redes sociales, exponentes claros de la estructura descentralizada, anárquica y abierta de la *web*. El desarrollo de los sitios de redes sociales ha estimulado la yuxtaposición entre identidades y contenidos publicados y ha contribuido a llevar al espacio público el tono y los temas de las conversaciones comunes. El lenguaje de las redes y las costumbres de publicación han subvertido también el control del contenido. El lema parece ser "publicar primero, filtrar después".

En pocos años, las plataformas de redes sociales conquistaron un lugar central, no solo en los usos de Internet sino en nuestras vidas, relaciones de amistad y de amor. Internet se convirtió en un inmenso patio de recreación.[5] En 2018 el nivel de penetración de las redes sociales a nivel mundial alcanza al 42%. En Argentina llega al 76%. El crecimiento promedio mundial de usuarios de redes alcanza al 13%, y en Argentina llega al 10%. El tiempo promedio diario que un/a argentino/a pasa en las redes sociales equivale a 3 horas y 9 minutos.

Las redes sociales se convirtieron en el espacio privilegiado de actuación dentro de la *web*. Eso significó que la democratización del espacio público que representó la aparición de Internet se trasladó al ámbito privado. La masificación y democratización resultado de la simplicidad en el acceso y uso de las redes sociales impone tensiones múltiples a la vez que superpone y sobrepone dilemas previos a Internet. Siempre que uno sea capaz de recordar cómo eran los tiempos previos.

- Libertad vs. Responsabilidad
- Control vs. Publicidad

4. Ídem.
5. Ídem.

- *Software* libre vs. Licencias de producto
- Publicidad vs. Intimidad
- Identidad vs. Anonimato
- Realidad vs. Virtualidad

La novedad de Internet es que dilemas tradicionales se revelan como falacias y otros emergen como contrastes que no necesariamente suponen una antítesis. Internet subvierte la antítesis aunque no ofrece síntesis. Ese breve listado de *versus* lejos está de ser exhaustivo. Solo pretende proponerle al lector visualizar la yuxtaposición de conflictos que no permiten trazar una divisoria clara. Lo difuso de Internet impone en el mundo de la legislación y la justicia la dificultad de cambiar el prisma de la interpretación.

Internet es democrática y democratiza. La aparición de nuevos riesgos derivados de la masificación y de la condición de anonimato que permite exige repensar y redefinir las regulaciones. Debemos, no obstante, ser prudentes. El exceso de regulación, la sobreregulación sobre usos permitidos, sobre modalidades de acceso, entre otros elementos, alterará la característica anárquica que tiene la www. Modificar esa característica traerá nuevas consecuencias imposibles de prever al momento de producir el cambio.

Los cambios que introduzcamos en favor de la seguridad y de la protección de los datos y usuarios deben ser progresivos, paulatinos y por sobre todas las cosas no deben estar guiados por el simple imperativo de la prohibición.

Convivencia digital

La masificación de Internet: ¿nueva herramienta o nuevo conflicto?

Las pantallas están en todos lados. Se hace imposible poder controlar todo el tiempo lo que un niño hace con sus dispositivos. Pero ¿es una solución quitarles las pantallas o limitar su uso?, la respuesta a esa pregunta es *no*. Tanto los chicos y los adolescentes –principalmente– como los adultos estamos en estado *online* a toda hora. En todos los casos, Internet es el principal método de interacción y de contribución al

desarrollo social; y hoy en día, para los más chicos significa una herramienta educativa muy importante, así como para los más grandes significa una herramienta para su trabajo. Con esto podemos concluir que en *esta nueva generación digital, en cada etapa de la vida, el uso de Internet mediante los distintos dispositivos es fundamental para el desarrollo.*

Ahora bien, ¿cuál es la solución para asegurar a nuestros hijos respecto al uso de Internet? Como dijimos, no es una solución la prohibición ni la limitación; pero sí lo es el uso responsable. Quitarles sus dispositivos implicaría que ellos dejen de tener la posibilidad de convivir en un estado en el que sus pares viven navegando, el *estado online*. Implicaría alejarlos de su círculo y probablemente eso desencadene el aislamiento del menor.

Por más que estén un paso más adelante los chicos, los "nativos digitales", nosotros también convivimos en este mundo *online-offline*. Es por eso que van aquí una serie de buenas prácticas que reuní para tener en cuenta a la hora de navegar en la red y en pos de promover el uso responsable de las redes.

Buenas prácticas

Asegurar mi anonimato en Internet

El derecho a la privacidad, en materia de comunicaciones, es fundamental que permanezca protegido. Resguardar la privacidad en Internet, puede ser una forma para ejercerlo. Hacerlo por completo es casi imposible, ya que cada dispositivo con el que nos conectamos a Internet va dejando múltiples huellas, más aun teniendo en cuenta que no solo lo hacemos desde las computadoras como en otros momentos, sino también desde celulares, tabletas, dispositivos de videojuegos, entre otros. Algunas de estas huellas son:

- Direcciones IP.
- Números de serie, sistemas operativos, navegador y toda información sobre nuestros computadores.
- Información de sesión o *cookies* y toda forma de rastrear en sitios *web*.

Estas son algunas soluciones para no entregar esta información:

- Servidores VPN o TOR, que entre otras cosas logran que no se relacione nuestra IP con nuestra identidad.

- TAILS u otros sistemas operativos que estén especialmente diseñados para la seguridad.
- Utilizar los modos privados en los navegadores de sitios *web* (como por ejemplo modo incógnito en Google Chrome) y desactivar *cookies* y otros complementos que faciliten la revelación de identidad.

Resguardar mis comunicaciones privadas por Internet

Como todos sabemos, el contenido de nuestras redes o de cualquier método de comunicación está a la vista y disposición de todo aquel que tenga un poco de paciencia y un mínimo conocimiento técnico.

Es así como todo contenido de nuestras redes sociales, correo electrónico, chats y distintos servicios puede ser atrapado y hasta intervenido si no están implementados los mecanismos de seguridad suficientes.

La principal recomendación en estos casos es verificar que estos sitios, así como también los proveedores de sistemas bancarios por ejemplo, usen sitios *web* seguros con el *https://* en su inicio, lo cual impide que terceras personas vean el contenido de la comunicación.

De todas formas, nuestros mensajes también suelen quedar almacenados en los mismos servicios. Por más que naveguemos de manera anónima o privada y que los sitios usen los mecanismos de navegación segura como el que mencionamos con anterioridad, el proveedor del servicio dispone de estos contenidos, puede leerlos y utilizarlos, como así también organismos gubernamentales relacionados principalmente con temas de seguridad.

Es por esto que, si necesitamos requerir un nivel más alto de confidencialidad (por información sensible o reservada), se recomienda implementar sistemas seguros de comunicación, donde se proteja, además, el contenido del mensaje.

Seguridad y cuidado de mis datos personales

Es importante tener en cuenta que cuando uno sube información o algún contenido a otro servicio *web*, *se pierde el control sobre este*. Estos son algunos consejos para poder lidiar con esto de la mejor manera:

1. Informate sobre los antecedentes del sitio. ¿Es conocido? ¿Hubo algún problema con la justicia en materia de protec-

ción de datos personales? ¿La gente lo recomienda en los distintos foros?

2. Revisá los términos y condiciones del servicio. Al crear un usuario en cualquier servicio *web* o plataforma, *siempre solicitan que aceptes antes de ser usuario los términos y condiciones del sitio así como las políticas de privacidad*. Si no podés interpretarlos por el léxico complejo que suelen utilizar o no podés ver la "letra chica", buscá referencias en Internet para poder comprenderlo.
3. ¿Es necesario que entregues toda la información personal que solicitan? Esto varía en los distintos sitios. Deberás revisar si es necesario entregar esa información para los fines requeridos.

Contenidos y publicaciones en redes sociales

Las distintas redes sociales como Instagram, Twitter, Facebook y muchas otras son un gran espacio para ejercer distintos derechos como nuestra libertad de expresión y compartir contenidos al respecto con nuestros usuarios amigos. Sin embargo, en estas redes, inevitablemente revelamos cosas de nosotros: qué estamos haciendo, dónde estamos, con quiénes estamos y demás.

Esto normalmente va acompañado de fotografías, datos geográficos y muchas veces de descripciones detalladas por nosotros de las actividades que realizamos y los dispositivos que utilizamos. Toda esta información se almacena en estos servidores y no podemos controlarla.

- *Primer consejo:* si querés que nadie se entere de estas cosas, no las subas en tus redes. No hay nivel de privacidad que supere la precaución.
- *Segundo consejo:* tené en cuenta que lo que hoy publiques o compartas, te puede seguir el resto de tu vida. Por lo tanto, pensá bien qué compartís y con quiénes.
- *Tercer consejo:* restringí el acceso a quienes no quieras que accedan a tu información. Esto podés hacerlo mediante los filtros de privacidad de las distintas redes sociales, donde por ejemplo podés seleccionar entre amigos, público, para grupos, entre otras.

Cuidá los datos de los usuarios de tu sitio *web*

Si sos dueño de algún sitio *web* y podés recoger algunos datos de tus usuarios (como por ejemplo las direcciones IP, *cookies*, comentarios y demás), tu deber legal es cuidar su privacidad.

En primer lugar, tenés que comunicar este hecho a los visitantes de tu sitio. Podés hacerlo a través de una política de privacidad que permita entender qué datos se recogen y con qué propósito. Además es recomendable implementar buenas prácticas para el uso de esta información:

- Evitar la solicitud de datos que son innecesarios para los fines del sitio, como número de documento o domicilios, a menos que realmente sean imprescindibles.
- Explicar para qué vas a utilizar esa información y respetar ese compromiso.
- No entregar a terceros esa información sin que el dueño de los datos personales lo autorice.
- Si es una autoridad o un organismo estatal quien lo solicita, entregalo solo cuando exista una autorización judicial o cualquier sello o firma la cual pueda certificarlo.

De todas formas, no olvides que la protección de la vida privada es un derecho fundamental y que la forma que dota de más legitimidad a la autoridad es una autorización judicial.

Manejar correctamente los comentarios en sitios *web*

Si sos administrador de un sitio *web*, seguramente tengas que lidiar con los comentarios de los usuarios. En muchas ocasiones, el contenido de aquellos puede ser controvertido por distintas razones, como por ejemplo:

- Insultos a otras personas.
- Discursos de odio o racismo.
- Contener promociones no deseadas o *spam*.
- Contenidos delictuales.
- Pornografía o contenidos no recomendables para menores de edad.
- Pornografía infantil.

En estos casos, es recomendable contar con una política de moderación de comentarios que establezca de forma clara qué contenidos son permitidos en el sitio o en qué casos los mismos serán removidos o censurados, pero sin olvidarse de que hay que tener en cuenta el derecho de libertad de expresión, por lo cual eliminar el contenido de manera arbitraria siempre será la *ultima ratio*.

Conclusión

Internet no es un problema, es una herramienta y un nuevo espacio donde hay que aprender a convivir. Y como dijimos, simplemente hay que aprender a utilizar esta nueva herramienta teniendo en cuenta los riesgos y facilidades que conlleva su uso, así como también hay que aprender a respetar e implementar las normas que existen en este espacio.

Así como convivimos de manera *offline*, hay que aprender a hacerlo de manera *online*.

¿Nuevos derechos "digitales" o los mismos derechos en un medio distinto?

Esta cuestión sigue generando controversias. Si bien hoy en día la gran mayoría sostiene que existen "derechos digitales", muchos otros consideran que los derechos son los mismos, pero lo que muta es el medio.

Es importante tener en cuenta que si hablamos de nuevos derechos, también hablamos de nuevas obligaciones. Y que los mismos no han sido contemplados en la Constitución Nacional. Ahora bien, si sostenemos la existencia de nuevos derechos, ¿cuáles serían ejemplos de estos? Los más importantes son los siguientes:

- Derecho a la libre expresión.
- Derecho a la privacidad en línea (*privacy online*).
- Derecho al acceso al ciberespacio (acceso a Internet) independientemente de las distintas características de los usuarios y de sus niveles de ingreso.
- Derecho a asociarse en comunidades en línea (conocidas también como comunidades virtuales).

- Derecho a compartir contenido.
- Derecho a la neutralidad de la red.

Además de los mencionados, hay un nuevo derecho que está en boga y que está relacionado con el hábeas data y la protección de datos personales: estamos hablando del *derecho al olvido*. El debate sobre tal derecho, fue ganando protagonismo, especialmente en Europa.

Esta discusión se da, principalmente, por una decisión del Tribunal de Justicia de la Unión Europea (en adelante TJUE) en el año 2014. El marco en el cual se da esta discusión es en materia de protección de datos personales. El TJUE decidió que Google y los distintos buscadores en general son "responsables" por el tratamiento de datos personales que aparecen en sus sitios *web*.

Por lo tanto, una definición de "derecho al olvido" podría ser la siguiente: es la facultad de que dispone cada persona (por ende titular de sus propios datos) para que cierta información que se encuentra accesible públicamente sea borrada o bloqueada por considerarse tal información obsoleta para el fin con el que se publicó y que sigue, de alguna manera, afectando al desarrollo personal de los ciudadanos.

Entonces, según este fallo llamado "Google Spain", una persona puede solicitar que una información personal que es inadecuada o excesiva sea removida de los resultados de las búsquedas, siempre que no exista interés público. El gestor de un motor de búsqueda, por lo tanto, está obligado a eliminarla.

El Centro de Estudios en Libertad de Expresión y Acceso a la Información señala tres grandes problemas que traería esta solicitud –que de todas formas no sienta jurisprudencia fuera de Europa– quienes lo consideran una mala solución:

- *Conflicto con derechos fundamentales como el acceso a la información y la libertad de expresión*. La decisión del tribunal europeo habla de la necesidad de buscar "un justo equilibrio" entre el derecho a la protección de datos personales y "el interés legítimo de los internautas potencialmente interesados en tener acceso a la información en cuestión".

  De todas formas, más adelante en ese mismo párrafo, señala que: "ciertamente, los derechos de esa persona [la que ve vulnerado su derecho a la privacidad por esos contenidos y pide al buscador ser 'desindexada'] prevalecen igualmen-

te, con carácter general, sobre el mencionado interés de los internautas". A la hora de pensar en legislación en Argentina, hay que tener en cuenta las particularidades y diferencias entre el marco europeo de protección de datos personales, y el sistema interamericano de protección de derechos y su robusto hincapié en el fortalecimiento del derecho a la libre expresión. Trasladar el abordaje europeo al marco regulatorio argentino (y de América Latina, en general) por ejemplo, podría entrar en conflicto con la prohibición de censura previa contemplada en el artículo 13 de la Convención Interamericana sobre Derechos Humanos. Si bien excede los objetivos de este trabajo, es un tema a tener en cuenta y que merece un análisis en profundidad a la hora de pensar en regulación en la materia.

- *Herramienta de censura en manos de privados*. Esta es de las cuestiones más preocupantes de la decisión del tribunal europeo. La persona interesada en eliminar un enlace de un buscador, según el fallo, puede presentar esas solicitudes directamente al gestor del motor de búsqueda, que deberá entonces examinar debidamente si son fundadas. Es decir, esta "solución" deja en manos de actores privados –de Google y del resto de los buscadores– la decisión final sobre a qué información y a qué contenidos podemos acceder en Internet. Una compañía termina ejerciendo un rol judicial y ni los usuarios ni los generadores del contenido son consultadas/os.
- *Desincentivos económicos y en desmedro de los intermediarios más "pequeños"*. Este tipo de decisiones parecen difíciles de implementar para las empresas más pequeñas que actúan como intermediarios. A todas luces, una compañía como Google puede destinar tiempo y dinero a revisar los pedidos de desindexación. Pero, ¿qué ocurre si este tipo de decisiones obligan también a generadores de contenidos y a otros buscadores y plataformas que no cuentan ni con los recursos ni con el *staff* de asesores legales de las compañías más poderosas?

Como dijimos, el "derecho al olvido" es materia de protección de datos personales. Si bien la Ley argentina N° 25326 quedó desactualizada por los avances tecnológicos, esta tiene un proyecto de ley que avanza

bastante en la materia. Si bien no voy a ahondar mucho en el tema, comparto el comentario de la ONG ADC al respecto:

> En primer lugar, queremos resaltar que la propuesta constituye un marco más adecuado para afrontar los desafíos que la presente realidad tecnológica le impone a los individuos. La necesidad de actualizar la legislación vigente es un anhelo que goza de un consenso general y en consecuencia, consideramos que este anteproyecto cumple con la exigencia de modernizar las normas a aplicar. En este sentido, destacamos la ampliación del catálogo de definiciones, ya que permitió incorporar conceptos –como los de computación en la nube, datos biométricos, datos genéticos, grupo económico, servicios de telefonía, servicios de la sociedad de la información y otros– que pertenecen a nuestro actual ecosistema digital.
> En segundo lugar, destacamos el hecho de que numerosas disposiciones se ajustan a los estándares más avanzados que existen en materia de protección de datos personales. Por un lado, la extensión de los principios y el mayor desarrollo del contenido de los derechos constituye una oportunidad para ampliar la protección del individuo frente a posibles abusos en el tratamiento de sus datos. Por otro lado, la adopción de institutos novedosos como el delegado de protección de datos, la evaluación de impacto o la privacidad por diseño y por defecto constituyen herramientas que pueden contribuir a incrementar la función preventiva del derecho de la protección de datos, evitando el daño antes de que se produzca.
> En tercer lugar, queremos destacar que el tratamiento del derecho de supresión fue realizado de manera equilibrada, buscando la ponderación de todos los derechos involucrados y mencionando expresamente la necesidad de proteger la libertad de expresión e información.
> En cuarto lugar, saludamos que se hayan tomado en cuenta varias de las sugerencias que nuestra organización realizó al momento de ser convocada para consulta. En ese sentido, la delimitación clara del ámbito de aplicación –para incluir el tratamiento que bases ubicadas en el extranjero realizan sobre datos de personas residentes en nuestro país– son muestra de un esfuerzo por ampliar la esfera de responsabilidad a sujetos que actualmente manejan grandes cantidades de datos personales. Asimismo, la no inclusión de las personas jurídicas como titulares de los derechos resulta coherente con el fuerte vínculo que la protección de datos tiene con el resguardo a la privacidad y a la intimidad.

Ciberdelitos

Los delitos frente a los nuevos conflictos sociales: ¿ciberdelitos, aggiornamiento de los tipos penales o ambos?

> ... nuevamente las tecnologías informatizadas generan nuevos dilemas, ya que estaríamos ante casos de ciberdelincuencia. Los ciberdelitos engloban en primer lugar dos cuestiones primales: la primera es la generación de nuevos tipos de delitos relacionados a los sistemas informáticos y la propia plataforma que estos ofrecen; y la segunda se refiere a delitos clásicos realizados mediante el uso del medio informático como instrumento de las acciones típicas.[6]

La Ley N° 26388 determinó qué tipo de conductas que emplean el uso de medios informáticos se constituyen en delitos para nuestro ordenamiento jurídico. Sin embargo, su dictado no fue suficiente para concluir con la dicotomía de si nos encontramos ante la presencia de nuevos delitos o por el contrario, se trata de viejos delitos previstos en nuestro Código Penal para los cuales sus autores utilizan la informática y la tecnología de la información para llevarlos a cabo. Una vez más Internet nos exige revisar lo "viejo" y lo "establecido" antes de caer innecesariamente en la calificación de "novedoso" y por tanto exento de regulación.

La amplia discusión dada entre juristas y doctrinarios probablemente continuará. Por ello y en favor de la simplicidad, debemos ceñirnos a lo que dispone la ley vigente.

Las conductas típicas incorporadas a nuestro Código Penal son:

- El uso de un medio informático para la producción, financiación, ofrecimiento, comercialización, publicación, facilitación, divulgación o distribución de *pornografía infantil* (art. 128 CP);
- La apertura, acceso, apoderamiento, supresión o desviación indebida de una *comunicación electrónica* (art. 153 CP);
- El *acceso* sin la debida autorización o excediendo la que posea a un *sistema informático* de acceso restringido (art. 153 *bis* CP);

6. Conf. Sentencia Nº 49 del 8 de mayo de 2017 del Juzgado de Menores de San Fernando del Valle de Catamarca en la causa Expediente Nº 75/2017, del 8/05/2017, caratulado "Informe remitido por la Dirección de Inteligencia Criminal de Policía de la Provincia s/ prevención del suicidio – desafío La ballena azul".

- La *publicación* indebida de una *comunicación electrónica* no destinada a la publicidad, si el hecho causare o pudiere causar perjuicios a terceros (art. 155 CP);
- El funcionario público que *revelare datos* que por ley deben ser secretos (art. 157 CP);
- *Acceder, proporcionar, revelar, insertar o hacer insertar* ilegítimamente *datos en un banco de datos personales* o violando sistemas de confidencialidad y seguridad de datos (157 *bis* CP);
- La *defraudación* mediante cualquier técnica de manipulación *informática* que altere el normal funcionamiento de un sistema informático o la transmisión de datos (inc. 16 art. 173 CP);
- La alteración, destrucción o inutilización de *datos, programas o sistemas informáticos*; la venta, distribución, hiciere circular o introdujere en un sistema informático, cualquier *programa* destinado a causar *daños* (art. 183 CP);
- La *interrupción o entorpecimiento de una comunicación* de cualquier naturaleza o *resistiere violentamente el restablecimiento de la comunicación interrumpida* (art. 197 CP);
- La *sustracción, alteración, ocultamiento, destrucción o inutilización* en todo o en parte de *objetos destinados a servir de prueba, registros* o documentos confiados (art. 255 CP).

Se puede advertir en esta enumeración que la incorporación dispuesta por la ley hace referencia al modo o medio utilizado por el autor para cometer la acción típica, lo que nos muestra que no necesariamente estamos hablando de desconocidas conductas típicas anteriores a esta norma. Es decir, los actos delictivos se cometen independientemente del soporte tecnológico.

A estos delitos debemos agregar otros que fueron aprobados por otras normas e igualmente incorporados al Código Penal, cuya relevancia es vital para nosotros en virtud de la figura de la víctima. Estamos hablando de delitos en los cuales la figura de la víctima recae sobre un menor de edad.

Consideramos de gran importancia estos delitos puesto que el daño causado a un menor lo marca para toda la vida. Por ello, el Estado en sus múltiples ámbitos debe prever estas circunstancias, desde la prevención hasta la condena de estas conductas.

Es así que el delito de *ciberacoso* a un menor o *grooming* que la Ley N° 26904 incorporó al texto del Código Penal (art. 131 CP), tiene como fin la protección de los menores ante la conducta de adultos que vulneran su integridad sexual.

Debemos tener en cuenta que si bien la conducta típica tiende a proteger este bien jurídico, la realidad es que con la incorporación de este delito al cuerpo normativo se trata de proteger incluso la vida del menor.

Porque aquí radica la relevancia de este delito. Que comienza como un delito al que podríamos denominar "menor" pero que puede escalar al delito más grave que prevé nuestro ordenamiento jurídico, que es aquel que protege el bien jurídico "vida". Innumerables casos ocurridos en nuestro país han demostrado que ello es así.

De igual modo es importante remarcar el reconocimiento como sociedad, más allá de las posibles discrepancias que se puedan tener respecto a su redacción y/o pena impuesta, de que la simple tenencia de pornografía infantil debía ser tipificada puesto que ese es el comienzo de un camino que puede escalar a niveles tan altos de delincuencia que comprende el ámbito internacional y que hasta puede derivar en el grave delito de trata.

La incorporación dispuesta por la Ley N° 27436 hoy permite investigar y condenar conductas que claramente tienen su origen en una conducta que debía ser reprochada por el ordenamiento penal.

¿Por qué hacemos esta afirmación? Porque para generar ese tipo de representaciones o participaciones primeramente debieron ser utilizados los menores para ese propósito. ¿Qué queremos decir con esto? Que el comienzo de la "simple tenencia" de la representación de actividades sexuales explícitas de un menor de dieciocho años, la organización de espectáculos con ese fin y la representación de sus partes genitales con fines sexuales en la generalidad de los casos se motivan en un aprovechamiento por parte del adulto sobre el menor así como el menoscabo de su integridad sexual.

Podrán decir que esas representaciones pudieron haberse originado entre menores adolescentes, por ejemplo, con consentimiento y sin la intervención de un adulto. Sin embargo, el simple hecho de que esas imágenes o filmaciones pasen a manos de un adulto conlleva a pensar necesariamente en la potencial comisión de delitos de gran escala. Y si bien nuestro ordenamiento jurídico no tipifica las simples

ideas o actos preparatorios, y de hecho es lo que han reafirmado nuestros legisladores con el dictado de esta ley, estamos convencidos de que con esta incorporación al Código Penal se allanarán las investigaciones originadas en la utilización de pornografía infantil, en todas las formas previstas en el primer párrafo del artículo 128 del Código Penal, mediante el uso de las redes.

La jurisprudencia ante los cambios

La jurisprudencia de nuestro país va amoldándose a las nuevas modalidades de relacionamiento o vinculaciones electrónicas. Estos cambios impactan al momento de investigar, analizar y resolver los conflictos e intereses que se encuentran en juego. Los magistrados enfrentan, por lo tanto, un nuevo imperativo a la hora de tomar decisiones: *la adaptación dinámica al contexto*.

Los cambios imponen a los magistrados adaptarse dinámicamente a estas circunstancias o hechos al momento de investigar, analizar y resolver los conflictos e intereses que se encuentran en juego.

A modo de ejemplo, citaré a continuación algunos fallos respecto de los diferentes tipos enunciados donde se evidencia la complejidad y desafíos que afrontamos no solo desde el Poder Judicial, sino como sociedad.

Las mismas se corresponden tanto con cuestiones penales como civiles o comerciales, y demuestran que la afectación y vulneración de derechos no se limita a ningún tipo de competencia o jurisdicción específica.

Secuestros virtuales: ¿estafa o extorsión?

Los secuestros virtuales son modalidades delictivas que se desarrollan hace ya varios años y que exigieron replantear la tipificación penal atento a sus características de "virtualidad".

Hoy en día aún no es pacífica la jurisprudencia en el tipo penal sobre estos hechos ya que mientras algunos magistrados lo encuadran en el delito de estafa (art. 172 CP), otros lo hacen como extorsión (art. 168 CP).

La Cámara Federal de San Martín, Sala II, Secretaría Penal Nº 2, mediante Resolución del 16 de agosto de 2011 dictada en la causa "Rocha Osvaldo Walter, Sudeyra Norverto Carlos y Negrete Octavio Damián s/ art. 168 y 210 del CP" confirmó el procesamiento de tres acusados por los delitos de extorsión reiterada en siete oportunidades –dos he-

chos consumados y cinco tentados–, en concurso real con el delito de asociación ilícita, en una causa por los llamados "secuestros virtuales".

Mientras que en otros hechos de características similares se ha entendido que se configura el delito de extorsión:

> ... la exigencia dineraria realizada, enmarcada en amenazas y simulando un secuestro, forman parte de una maniobra ardidosa tendiente a afectar el psiquismo del destinatario como para hacerlo incurrir en un error o inducirlo a concretar la disposición patrimonial pretendida. Se aleja así la ilícita pretensión del concepto de intimidación que requiere la extorsión, pero se configura uno de los elementos tipificantes del delito de estafa prevista en el artículo 172 del Código Penal y en relación a ella debe evaluarse la idoneidad que se atribuyó a la conducta desplegada por la encausada.[7]

Phishing

El *phishing* es una maniobra de fraude mediante la técnica de manipulación informática y hoy en día es uno de los tipos de fraude *online* o vulneración de ciberseguridad más frecuentes.[8]

A nivel internacional y en materia de seguridad su definición o término informático comprende a los abusos cometidos mediante el uso de ingeniería social para adquirir información confidencial en forma fraudulenta (como puede ser una contraseña, información detallada sobre tarjetas de crédito u otra información bancaria) e incluso la lectura por parte de terceras personas, de las letras o números que se marcan en nuestros equipos como celulares o computadoras.

Ahora bien, nuestro sistema penal comprende esta modalidad en la tipología del artículo 173, inciso 16 del Código Penal (incorporado por Ley N° 26388) que estipula que para que se configure el delito de estafa informática deben darse tanto el supuesto del ardid o engaño, como el perjuicio patrimonial consecuente con ese engaño.

Esta situación en la Argentina exige que los operadores y magistrados deban analizar con mucho detenimiento y cautela estas conductas tendientes a conseguir y obtener información de datos,

7. Cámara Nacional de Apelaciones en lo Criminal y Correcccional, Sala I, CCC 52203/2017; "M.,S.G. procesamiento". Resolución del 11 de octubre de 2017.

8. "Argentina, entre los países que más *phishing* reciben en el mundo", en diario *Clarín*. Disponible en: http://www.clarin.com/sociedad/argentina-paises-phishing-reciben-mundo_0_SkrEtz1kM.html

productos de los engaños para que estas conductas encuadren la tipología penal que resulte aplicable.

La Cámara de Casación Penal de la Capital Federal, Sala III, con fecha 16 de junio de 2015 en la Causa Nº CCC 51772/2011/TO1/CFC1 "Castelo, Pablo Alejandro s/recurso de casación" confirmó la condena del delito de defraudación mediante técnicas (art. 173 inc. 16 CP), ya que el condenado "mediante la manipulación indebida de datos informáticos obtuvo el usuario y contraseña" de la víctima y titular de la cuenta del Banco Francés, "para luego efectuar una transferencia de capitales mediante el sistema '*home banking* Francés-net' por la suma de pesos" hacia otra cuenta bancaria desde la cual el dinero fue retirado.

Este fallo mantiene el criterio sentado en la Causa "G.R. y otro s/ procesamientos" (Causa N° 39.779), donde la Sala VI de la Cámara Nacional de Apelaciones en lo Criminal y Correccional el 3 de agosto de 2010 confirmó el procesamiento por el delito conocido como *phishing* por la obtención de datos de tarjetas de crédito para transferir a otra cuenta bancaria de los procesados.

Recientemente, el Superior Tribunal de Justicia de Jujuy en una causa cuyos antecedentes enmarcan un clásico caso o modalidad de *phishing* resolvió un resarcimiento civil.

Con fecha 22 de mayo de 2017, en la causa "Ordinario por daños y perjuicios: Salum, Andrés Alejandro c/ Banco Santander Río S.A." el Tribunal confirmó la responsabilidad de la entidad bancaria ordenando resarcir al actor (titular de cuenta bancaria y damnificado) considerando lo siguiente:

> … que, en función de la "responsabilidad objetiva", el Banco incumplió con la prestación comprometida (custodiar el dinero que el actor le había entregado en depósito) pues lo había entregado por uno de sus canales de pago (cajero automático) a un tercero que no era el titular de la caja de ahorro, ni tampoco tenía autorización para hacerse de esos fondos.
>
> … ante un supuesto de responsabilidad objetiva (obligación de resultado) poco importaba lo que experto hubiera concluido con relación a la permeabilidad del sistema de seguridad implementado por el Banco demandado, ya que este –ante el contrato de caja de ahorro celebrado con el actor– simplemente debió resguardar los fondos que le fueron confiados en custodia, cosa que evidentemente no hizo; parte de los mismos fueron fraudulentamente extraídos, al margen del grado de confiabilidad que

> pudo tener el sistema. De hecho, ni al accionante, como cliente damnificado por la sustracción de su dinero, ni tampoco al Juez les puede interesar si el sistema de seguridad era infalible; lo cierto es que el Banco debe responder ante esa indebida detracción de fondos, más allá de lo que pudo llegar a concluir el Perito. Y tan es así que la verdadera víctima de los "piratas informáticos" fue la entidad bancaria y no el Sr. Salum, porque fue a ella a quien burlaron y quebrantaron las medidas de seguridad que dice haber implementado e invoca como eficientes; circunstancias estas que –reitero– no hacen a resolución del caso y por ello la razonable decisión del Tribunal *a quo* en no producir una prueba inconducente.

Este antecedente expone la complejidad con la que hoy se deben analizar los hechos y el rol de las víctimas y damnificados a la luz de la interpretación sistemática e integral del derecho.

Acceso ilegítimo a una "comunicación electrónica" o "dato informático de acceso restringido"

El Código Penal en el artículo 153 reprime con prisión de quince días a seis meses

> ... al que abriere o accediere indebidamente a una comunicación electrónica, una carta, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, que no le esté dirigido; o se apoderare indebidamente de una comunicación electrónica, una carta, un pliego, un despacho u otro papel privado, aunque no esté cerrado; o indebidamente suprimiere o desviare de su destino una correspondencia o una comunicación electrónica que no le esté dirigida.

Además, incorporó el artículo 153 *bis*, que fija la misma pena "si no resultare un delito más severamente penado", al que "a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido".

Si bien no hay unidad de criterio sobre los accesos sin permisos del propietario en las redes sociales, la Corte Suprema de Justicia de la Nación ha intervenido en contiendas de competencia sosteniendo como doctrina que el acceso ilegítimo a una "comunicación electrónica" o "dato informático de acceso restringido", en los términos de los artículos 153 y 153 bis del Código Penal, según la Ley N° 26388, a los que "solo es posible ingresar a través de un medio que por sus características propias",

se encuentra dentro de los servicios de telecomunicaciones que son de interés de la Nación (en virtud de los arts. 2 y 3 de la Ley N° 19798), por lo que debe ser investigado por la justicia federal.

Así lo ha expresado recientemente en la causa "CSJ 658/2017; T,G.W. s/ violación de sistema informático (art. 153 *bis*, 1er Párr. del C.P.)" y "Carca, Gustavo Luis s/ denuncia violación de correspondencia".

A modo de ejemplo de este tipo de delitos podemos citar al fallo de la Sala I de la Cámara Federal de Casación Penal, de fecha 30 de marzo de 2017, donde se confirmó la sentencia dictada por el Juzgado en lo Criminal y Correccional Federal N° 2 de San Isidro, condenando a la pena de 10 meses de prisión de ejecución condicional por el delito de acceso ilegítimo a un sistema o dato informático de acceso restringido reiterado. Tratándose de un caso en el cual el imputado se había desempeñado como contador de una cooperativa –conociendo sus claves fiscales– y donde después de haber renunciado litigiosamente accedió desde un dispositivo a la página *web* de la AFIP, específicamente a los datos informáticos de la empresa y del querellante, utilizando para ello las claves fiscales asignadas a ambos sin su autorización.[9]

Grooming

El *grooming* es uno de los delitos cuya denuncia ha crecido exponencialmente a lo largo de los últimos años. Ello se debe no solo al incremento de los menores como usuarios –y en virtud de ello como posibles víctimas– a las redes sociales, sino a que se está tomando conocimiento y conciencia del riesgo que tiene implícito y con ello se instrumentan o formalizan las denuncias.

Este fenómeno se refiere a la práctica de un delincuente que crea una conexión emocional con un menor, con una finalidad sexual. Este delito informático consiste en adultos que buscan establecer lazos de amistad con menores en Internet, con el objetivo de obtener una satisfacción sexual mediante imágenes eróticas o pornográficas del menor y, en casos más extremos, esos vínculos pueden llegar a encuentros con consecuencias muy graves.

9. Cám. Fed. de Casación Penal, Sala I, Causa N° 32224. Querellado: Ranieli, Germán Walter s/violación sist. Informático art. 153 *bis* 1° párrafo. Registro N° 178/17.

El 19 de octubre de 2017 el Tribunal Oral en lo Criminal (TOC) N° 2 de Bahía Blanca condenó con prisión perpetua al hombre por engañar a una niña de 12 años mediante un perfil falso de Facebook, intentar abusar sexualmente de ella y asesinarla encuadrando en los delitos de *grooming* y femicidio.

El Tribunal Oral en lo Criminal y Correccional Nº 19 de la Capital Federal (CCC 63603/2016/TO1) con fecha del 26 de diciembre de 2017 condenó a un hombre calificando el hecho como la prevista en el artículo 131 del CP, llamada "*grooming*, *child grooming* o ciberacoso a menores", en tanto el imputado se contactó con la menor de edad, a través de las redes sociales vía conexión de Internet; con fines de carácter sexual vía "WhatsApp" (art. 131 CP) y en concurso ideal con el delito de coacción, toda vez que el acusado actuó con el propósito de obligar a la víctima a enviarle fotos, bajo amenaza de publicar una foto de una mujer desnuda alegando que sería ella (art. 149 *bis* CP).

Destaca respecto del *grooming* la amplitud o variedad de modalidades en la que puede configurarse y debe analizarse:

> Respecto a la acción típica de este delito la jurisprudencia tiene dicho que "es un acto preparatorio punible, en el que las modalidades de comisión pueden ser de lo más variadas: mensajes, imágenes, declaraciones de afecto, bromas procaces, etcétera. La acción u omisión implica un acercamiento con el objeto de establecer una relación de confianza, de poder y/o control emocional sobre el menor mediante la manipulación o el engaño en el que el adulto, sujeto activo, enmascara su identidad con la finalidad de que el niño o niña a través del vínculo establecido pierda sus inhibiciones y realice acciones de índole sexual. La interacción de al menos dos personas para que el delito pueda concretarse tiene su campo de acción en redes sociales –email, blogs, páginas, salas de chat, aplicaciones de mensajería, mensajes de texto SMS, llamadas, videollamadas, juegos en línea, etcétera–.

La sentencia –en virtud de la condena en suspenso– impuso una restricción de acercamiento a la menor y abstenerse de relacionarse con ella, por cualquier medio (físico, epistolar, telefónico, gestual o a través de las redes sociales de Internet).

Un poco más allá fue el fallo dispuesto por el Juzgado en lo Correccional Nº 2 de Bahía Blanca con fecha del 31 de marzo de 2017, en un caso de *grooming* en el que la víctima de 10 años recibió mensajes

de texto con contenido sexual del acusado, y se impusieron reglas de conducta en la condena de ejecución condicional:

> FALLO condenando al procesado R.A.A., cuyos datos personales obran en el veredicto precedente, como autor penalmente responsable del delito de ACOSO SEXUAL TECNOLÓGICO DE MENORES, en los términos del art. 131 del Código Penal, cometido los días 26 y 27 de junio de 2014 en esta ciudad de Bahía Blanca y en perjuicio de J. M. C.P. ; a sufrir la pena de UN AÑO DE PRISIÓN, que, por concurrir las circunstancias previstas por el art. 26 del Código Penal y en razón del efecto criminógeno que conlleva el cumplimiento de penas breves en establecimientos carcelarios inadecuados; APLICO COMO DE EJECUCIÓN CONDICIONAL, sujeta tal modalidad al cumplimiento de las siguientes reglas de conducta por el término de DOS AÑOS: l) Fijar residencia y someterse al cuidado del Patronato de Liberados, Órgano al que deberá comunicarse lo aquí resuelto para su debido contralor; 2) abstenerse de acercarse a menos de doscientos metros de J. M. C.P., su vivienda o el sitio en que se encuentre ocasionalmente; 3) *Abstenerse de utilizar telefonía celular o internet, para lo cual habrá de comunicarse tal inhibición a las compañías telefónicas habilitadas en la región*. Todo bajo apercibimiento de lo dispuesto en el art. 27 *bis* último párrafo del Código Penal con más el pago de las costas procesales (arts. 40 y 41 del Código Penal y 375, 376, 380, 530 y 531 del Código Procesal Penal).

Instigación al suicidio. Juegos peligrosos

Nuestro Código Penal en su artículo 83 tipifica los delitos de instigación y/o ayuda al suicidio. Si bien es muy complejo analizar esta situación, las nuevas formas de relacionamiento y accesos a las redes sociales hoy exigen una mirada o revisión al respecto.

Por eso, la resolución preventiva del 8 de mayo de 2017 dictada por el Juzgado de Menores de San Fernando del Valle de Catamarca, en el marco de una problemática social que quedó expuesta a través del denominado juego de "la Ballena Azul", merece su cita y transcripción:

> En nuestro país el día 02/05/17 en la provincia de San Juan se habría registrado el primer caso de un supuesto intento de suicidio por parte de un joven de 14 años al haber consumido un blíster íntegro de pastillas, quien lo hacía hasta el momento en la unidad de terapia intensiva del Hospital Rawson, que también tendría directa relación con la participación del adolescente en el "juego de la ballena azul"; tal es así que solo

horas antes habría modificado su estado de Whatsapp en dos oportunidades: en una expresaba "Jugando el juego de la Ballena Azul", y en otro "Adiós a todos. Los amo", este último junto a un emoji de un cuchillo y dos caras de tristeza. Por último en la ciudad de La Plata, provincia de Buenos Aires se confirmó la investigación de un caso de una niña de 12 años, que asiste al liceo de la Universidad Nacional "Víctor Mercante", a quien se le verificó la existencia de lesiones corporales en sus extremidades que serían compatibles con las que impone este peligroso juego...

Como podrá advertirse los actos suicidas desencadenados por el juego de "la ballena azul", no responden a la forma de concreción de las figuras colectivas mencionadas, las nuevas tecnologías informáticas han venido a cambiar no solamente la forma de comunicación e interacción de las personas (formas de comunicación interpersonales, redes sociales), sino también ha movido los parámetros a través de los cuales se desarrollaban actos de la vida cotidiana, comerciales y económicos (proliferación de sitios *online* de compra y venta, actividad mercantil y bancaria totalmente informatizada), jurídicos y administrativos (la concepción del trámite administrativo y jurídico *online*).
Sin embargo también ha servido de plataforma para actos con connotaciones plenamente dignas de reproche o sanción social y/o moral, como también de tipo punitivo según las legislaciones de cada país o estado; dentro de tales se sitúa el suicidio, por ende podríamos considerar en una primera aproximación que aquellas personas que deciden quitarse la vida como una consecuencia de haber utilizado el juego de "la ballena azul" como una especie de instrumento que dio nacimiento, o impulso o concreción a ideas autodestructivas.
Este fenómeno ha desarrollado un tipo de suicidio por imitación con las particularidades inherentes a las tecnologías 2.0, es decir se trataría de: 1 – individuos sin vínculo social pero que atraviesan un fenómeno psicológico similar (la adolescencia y su vulnerabilidad); 2 – sentido de pertenencia a un grupo, tal como lo evidencia la creación de grupos cerrados a través de las redes sociales donde se "reclutan" a los participantes; 3 – la imitación no es la causa de actos autodestructivos, sino es consecuencia de un proceso complejo compuesto por una transmisión psicológica que puede acarrear una epidemia suicida, 4 – condiciones sociales, culturales, y problemáticas afines entre desconocidos con una gran necesidad de sentido de pertenencia.

Es sumamente necesario advertir que nuestra provincia ostenta un elevado porcentaje de suicidio de NNyA, tal es así que en los últimos años

> ha ostentado ser la tercera provincia con mayor tasa de suicidio adolescente. Entre los años 2014 y 2015 se tomó conocimiento de verdaderos pactos suicidas entre adolescentes, los cuales tuvieron gran trascendencia en este tribunal ya que se trataban de jóvenes que registraban causas penales, varias aún en curso de investigación hasta ese momento.
>
> Por último, asimismo cabe destacar que este juzgado también ha intervenido respecto de un gran número de casos donde el resultado lesivo o dañoso se ha producido por la imitación por parte de NNyA de "juegos" o "desafíos" divulgados en las redes sociales, cuyas prácticas las han llevado adelante sin tener ningún tipo de conciencia ni magnitud sobre la peligrosidad de las mismas. Como el lamentable caso registrado el día 19/11/16 en jurisdicción de la Comisaría Seccional donde una adolescente de tan solo 12 años perdió su vida, al intentar imitar el juego denominado "bolas de fuego" –el cual había visto en YouTube–. La niña había sufrido quemaduras de tipo AB, y B que le produjeron un *shock* refractario luego de un síndrome de respuesta inflamatoria sistémica.

Es dable destacar que en su parte resolutiva, el magistrado dispuso notificar a la Subsecretaría de Salud y Adicciones del Ministerio de Salud de la Provincia de Catamarca para instar la aplicación y cumplimiento de la Ley provincial N° 5484 y nacional N° 27130 referidas a la prevención del suicidio, y resolvió que –a través de la Oficina de Prensa y Difusión de la Corte de Justicia– se publique en los periódicos de mayor tirada y relevancia de la provincia las pautas de detección y prevención del desafío llamado "La Ballena Azul", en el argumento del artículo 17 de la Convención Internacional de los Derechos del Niño.

Naturaleza, competencia y jurisdiccionalidad en la ciberdelincuencia

Debemos dejar de ignorar el crimen organizado en esta esfera. Es un deber que tenemos como Estado. El gran número de investigaciones que se originan en el Poder Judicial de la CABA y en todo el país, demuestran que el uso de las redes sociales, la tecnología y la informática en nuestros días facilitaron el acrecentamiento de estas conductas delictivas que llegan a escala internacional en primera medida y al crimen organizado como acción de mayor gravedad.

Tanto la Convención Internacional contra la Delincuencia Organizada Transnacional, aprobada por la Ley N° 25632 y el Convenio sobre Ci-

berdelito del Consejo de Europa, recientemente aprobado con algunas reservas por la Ley N° 27411, obligan a los Estados a crear herramientas de investigación y de reprobación de este tipo de conductas delictivas.

Si bien el Convenio sobre Ciberdelito fue aprobado por nuestro país en noviembre del año 2017, la realidad es que puede entenderse que parte de su contenido, específicamente hablamos de los delitos, fueron incorporados a nuestro ordenamiento penal con la Ley N° 26388.

Es cierto que este convenio fue dictado por el Consejo Europeo y que la Argentina no forma parte de él, sin embargo no se puede dejar de remarcar que esta fue una herramienta de gran utilidad para el resto de los países que no integran el Consejo, puesto que su contenido es abarcativo de las necesidades que deben cubrir los Estados para contrarrestar la cibercriminalidad.

De hecho, en el año 2014 el Consejo de Procuradores, Fiscales, Defensores y Asesores Generales de la República Argentina y el Consejo Federal de Política Criminal, crearon el Protocolo de Intervención Urgente y Colaboración Recíproca en casos de Detección de uso de Pornografía Infantil en Internet.

El documento contempló la instauración de la Red 24/7 que tiene como finalidad la actuación inmediata y la transmisión de datos necesarios a la jurisdicción que corresponda ante la denuncia y/o toma de conocimiento en una jurisdicción de la comisión de un delito de este tipo en otra. Esta actuación inmediata tiene como fin la urgente protección del menor víctima, así como la pronta intervención de la investigación judicial para evitar la pérdida de la prueba informática y el esclarecimiento del hecho.

En este protocolo tampoco se puede negar la influencia del Convenio sobre Ciberdelito que expresamente prevé este tipo de intervención de los Estados para el esclarecimiento de los delitos informáticos, así como la recolección de prueba electrónica.

Por otra parte, la preexistencia de la suscripción del Convenio entre Ministerio Público Fiscal de la CABA con el Centro Nacional para Niños Desaparecidos y Explotados (NCMEC), generó una primera herramienta para la investigación del delito de pornografía infantil.

A través de este convenio el Ministerio Público Fiscal de nuestra Ciudad implementó un sistema de comunicación a partir del cual, a través de una red virtual privada (VPN), reciben todos los reportes de pornografía

infantil detectados en el territorio nacional. Este convenio fijó los estándares para que la Fiscalía de la Ciudad pudiera establecer una conexión remota con la red y descargar y/o revisar los informes de *Cyber Tipeline*.

Sin embargo, a nuestro ordenamiento jurídico le falta mucho camino por recorrer para estar a la altura de las circunstancias de la modernidad delictiva, carece de herramientas procedimentales que permitan la intervención en tiempo oportuno en especial para la protección de los medios probatorios de este tipo de delitos. Esto conduce, muchas veces, a investigaciones de las cuales no se obtiene el resultado esperado.

Nuestro país debe seguir trabajando en la modernización de las leyes a fin de encontrarnos ante una actuación de la justicia en tiempo y forma. Y creemos también que este camino debe continuar en la cooperación internacional.

Bibliografía

ASOCIACIÓN POR LOS DERECHOS CIVILES (ADC), "Comentarios acerca del anteproyecto de ley de protección de datos personales", febrero de 2017. Disponible en: https://adcdigital.org.ar/wp-content/uploads/2017/03/Comentarios_leyPDP.pdf

BISQUERT, Sebastián Oscar, "La figura del 'phishing' como modalidad delictiva. Problemática en cuanto a su encuadre jurídico", 2006. Disponible en: http://www.saij.gob.ar/doctrina/dacf060096-bisquert-figura_phishing_como_modalidad.htm

BUOMPADRE, Jorge E., "¿Acoso sexual a menores por vía digital o castigo de los malos pensamientos?", *Revista de Derecho Penal*, N° 5, 2017 (referencia: IJ-CCCLXXVI-110).

CÁMARA DE CASACIÓN PENAL DE LA CAPITAL FEDERAL, "C., P. A. s/recurso de casación", Sala III, 2015, Expediente N° CCC 051772/2011/TO01/CFC001. Disponible en: http://www.cij.gov.ar/sentencias.html

CÁMARA FEDERAL DE CASACIÓN PENAL, "R., G.W. s/ violación sistema informático, art. 153 bis, 1° párrafo", Causa N° 32224, Sala I, sentencia del 30/032017. Disponible en: http://www.cij.gov.ar/nota-

25440-Casaci-n-Federal-ratific-condena-por-el-delito-de-acceso-ilegtimo-a-un-sistema-o-dato-inform-tico-restringido.html

CÁMARA FEDERAL DE CASACIÓN PENAL DE LA CABA, "C., P.A. s/recurso de casación", Causa N° 051772/2011/TO01/CFC001, Sala III, sentencia del 16/06/2015. Disponible en: http://www.pensamientopenal.com.ar/system/files/2015/07/fallos41472.pdf

CÁMARA NACIONAL DE APELACIONES EN LO CRIMINAL Y CORRECCIONAL, "M.,S.G. procesamiento", Sala I, Causa N° 52203/2017, sentencia del 11/10/2017. Disponible en: http://www.diariojudicial.com/public/documentos/000/077/152/000077152.pdf

CÁMARA NACIONAL DE APELACIONES EN LO CRIMINAL Y CORRECCIONAL DE LA CABA, "G. R. y otro s/procesamientos", Causa N° 39779, Sala VI, Juzgado de Instrucción N° 2, sentencia del 03/08/2010. Disponible en: http://www.delitosinformaticos.com.ar/pdf/fallophishing1.pdf

CAMMAERTS, Bart y VAN AUDENHOVE, Leo, "Online Political Debate, Unbounded Citizenship, and the Problematic Nature of a Transnational Public Sphere", en *Political Communication*, Vol. 22, N° 22, 2005.

CARDON, Dominique, *La democracia Internet. Promesas y límites*, Buenos Aires, Editorial Prometeo, 2010.

CASTELLS, Manuel, *The Internet Galaxy: Reflections on the Internet, Business, and Society*, Nueva York, Oxford University Press, 2001.

_____, *The Information Age. Economy, Society and Culture*, Oxford, Wiley Blackwell, 2010.

_____, *Comunicación y poder*, Madrid, Alianza Editorial, 2009.

CENTRO DE INFORMACIÓN JUDICIAL, "Secuestros virtuales: confirman procesamientos por los delitos de extorsión y asociación ilícita", 25/08/2011. Disponible en: http://cij.gov.ar/nota-7582-Secuestros-virtuales-confirman-procesamientos-por-los-delitos-de-extorsi-n-y-asociaci-n-il-cita.html

CENTRO DE INFORMACIÓN JUDICIAL, "Casación Penal confirma condena por defraudación informática", 2015. Disponible en: http://www.cij.gov.ar/nota-16796-Casaci-n-Penal-confirm--condena-por-defraudaci-n-inform-tica.html

CHADWICK, Andrew, "Digital Network Repertories and Organizational Hybridity", en *Political Communication*, Vol. 24, N° 3, 2007.

CORTE SUPREMA DE JUSTICIA DE LA NACIÓN, "C. G.L. s/ Denuncia violación de correspondencia", sentencia del 25/04/2017. Disponible en: http://www.saij.gob.ar (ref.: Id SAIJ: FA17000023).

CORTE SUPREMA DE JUSTICIA DE LA NACIÓN, "T., G.W. s/ violación sistema informático art. 153 bis 1° párrafo", Causa N° 658/2017, sentencia del 19/09/2017. Disponible en: http://www.saij.gob.ar (ref.: Id SAIJ: FA17000077).

DELUCA, Santiago y DEL CARRIL, Enrique H., "Cooperación internacional en materia penal en el Mercosur: El cibercrimen", en *Revista de la Secretaría del Tribunal Permanente de Revisión*, N° 10, 2017 (referencia: IJ-CDLXXXIV-593).

DIARIO JUDICIAL, "Un nuevo caso de 'phishing' con la venta de pasajes *online*", 22/12/2016. Disponible en: http://www.diariojudicial.com/nota/77011

DIARIO JUDICIAL, "Un secuestro virtual con una acusación real", 09/02/2018. Disponible en: http://www.diariojudicial.com/nota/80075

ERREIUS, "Advierten sobre la necesidad de que el Código Penal regule los denominados 'secuestros virtuales'", 14/02/18. Disponible en: https://www.erreius.com/opinion/12/penal/Nota/32/advierten-sobre-la-necesidad-de-que-el-codigo-penal-regule-los-denominados-secuestros-virtuales

FERNÁNDEZ DOYAGUE, Amalia, "La denominada violencia cibernética. Internet y las redes sociales", 26/11/2014. Disponible en: http://www.abogacia.es/2014/11/26/la-denominada-violencia-cibernetica-internet-y-las-redes-sociales/

FERRARI, Verónica y SCHNIDRIG, Daniela, "Responsabilidad de intermediarios y derecho al olvido. Aportes para la discusión legisla-

tiva en Argentina", CELE, 2015. Disponible en: https://www.palermo.edu/cele/pdf/Policy_Paper_Derecho_al_Olvido.pdf

FIGARI, Rubén, *Reflexiones sobre la defraudación informática (ley 26.388)*, Buenos Aires, IJ Editores, 2012 (referencia: IJ-LI-748).

GONZÁLEZ PÉREZ, Leo, "Argentina, entre los países que más *phishing* reciben en el mundo", *Clarín*, 07/11/2017. Disponible en: https://www.clarin.com/sociedad/argentina-paises-phishing-reciben-mundo_0_SkrEtz1kM.html

JUZGADO DE MENORES Nº 1 DE SAN FERNANDO DEL VALLE DE CATAMARCA, "Informe remitido por la Dirección de Inteligencia Criminal de Policía de la Provincia s/ prevención del suicidio -desafío La ballena azul-", sentencia del 08/05/2017. Disponible en: http://www.saij.gob.ar (ref.: Id SAIJ: FA17300000).

JUZGADO EN LO CORRECCIONAL Nº 2 DE BAHÍA BLANCA, "R. A. A.", Causa Nº 3475, Expte. N° 3465, sentencia del 31/03/2017. Disponible en: http://www.scba.gov.ar/jurisprudencia/ActualidadPBA.asp?date1=2017-3-31&date2=2017-4-14&expre=grooming&id=1&cat=0&fuero=

LA NUEVA, "Llamativo fallo por *Grooming*", 01/04/2017. Disponible en: http://www.lanueva.com/nota/2017-4-1-7-59-0-llamativo-fallo-por-grooming

LEMAÎTRE PICADO, Roberto, "Persecución de los delitos informáticos desde la perspectiva informática", en *Revista Iberoamericana El Derecho Informático*, N° 7, 2011 (referencia: IJ-LXIV-729).

MIGLIORISI, Diego, "Los diez delitos informáticos más frecuentes en la República Argentina", guardado de dirección IP para investigar delitos informáticos, en *Revista Iberoamericana El Derecho Informático*, N° 22, 2016 (referencia: IJ-CCCLXXVII-556).

MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS DE LA NACIÓN, *Segundo muestreo de denuncias judiciales de la República Argentina año 2014*, Sain, Gustavo (dir.), Olaeta, Hernán (coord.), Buenos Aires, Ediciones SAIJ, 2017.

NIKLAS, Luhmann, *The reality of Mass Media*, Stanford University Press, 1995.

ONG DERECHOS DIGITALES. Disponible en: https://www.derechosdigitales.org/tipo_publicacion/publicaciones/

PESCAROLI CASADO, Aline Gabriela, "Cyber bulling: violencia virtual e o enquadramento penal no Brasil", *Ámbito Jurídico*, Rio Grande, XIV, Nº 95, 2011. Disponible en: http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=10882

Política Judicial, nota *online*, 2017. Disponible en: http://www.politicajudicial.com/un-fallo-de-la-corte-admite-que-violar-una-cuenta-de-facebook-encuadra-como-violacion-a-la-correspondencia/

REVISTA PENSAMIENTO PENAL, "Violación de correspondencia. Ingreso subrepticio a una cuenta de Facebook", 18/05/2017. Disponible en: http://www.pensamientopenal.com.ar/fallos/45334-violacion-correspondencia-ingreso-subrepticio-cuenta-facebook

ROSENDE, Eduardo E., "La aventura del proceso penal: problemas relacionados con el ejercicio de la acción y la competencia en los 'delitos informáticos'", en *Revista de Derecho Penal*, N° 1, 2015 (referencia: IJ-LXXVVVV-837).

TRIBUNAL ORAL EN LO CRIMINAL Y CORRECIONAL Nº 19 DE LA CABA, "M.J., R.A. s/acoso sexual a menores por comunicaciones electrónicas - art. 131 del C.P. y Coacción (art. 149 bis)", CCC 063603/2016/TO1, 2017. Disponible en: http://www.cij.gov.ar/sentencias.html

TRIBUNAL SUPERIOR DE JUSTICIA DE JUJUY, "Salum, Andrés Alejandro c/ Banco Santander Río S.A". Expediente CF-12591-2016, Libro de Acuerdos: 2, Registro Nº 102, Fº 417/424, 2017. Disponible en: http://www.justiciajujuy-juris.gov.ar:8081/frm_resultado_out_sentencias.aspx?id=287398

VON HIPPEL, Eric, *Democratizing Innovation*, Cambridge, The MIT Press, 2005.

WERNER, Matías, "'Phishing' con resarcimiento civil", en *Diario Judicial*, 2017. Disponible en: http://www.diariojudicial.com/nota/78646

Estrategias y planteos en casos de delitos informáticos. Desafíos para la Defensa

Yanina Gabriela Matas*

Introducción

Los avances tecnológicos y científicos transforman de manera constante la vida de la sociedad, por lo que el *sistema penal* también debe acompañar, íntegramente, esos cambios. Al referirme al *sistema penal* estoy haciendo alusión no sólo a las normas penales sino también a las reglamentaciones procesales, a las herramientas y procedimientos utilizados para la adquisición y conservación de la evidencia digital y, también, al modo de actuar de los operadores judiciales.

En el presente artículo pretendo poner de relieve sólo algunas de las tantas problemáticas con las que se encuentra, en primer lugar, todo el sistema judicial debido al abordaje puntual que presentan los denominados *delitos informáticos*. Seguidamente, con relación a esas dificultades, realizaré un análisis somero de las normas procesales penales que enmarcan el procedimiento que se debe llevar a cabo en cuanto a la actividad probatoria, particularmente las del Código Procesal Penal de la Ciudad. Luego, pondré en evidencia algunos de los problemas puntuales a los que debe enfrentarse el Ministerio Público de la Defensa a la hora de elaborar una estrategia en los casos en los que su asistido esté imputado de la comisión de un delito informático.

Finalmente, a partir de un relevamiento preliminar de casos del fuero Penal, Contravencional y de Faltas de la CABA, mencionaré las respuestas jurisdiccionales que se fueron brindando, en las distintas instancias, a los planteos efectuados por las partes.

---

* Especialista en Derecho Penal (UBA), maestrando en Derecho Penal (UBA). Profesora Ayudante de segunda en la materia Derecho Contravencional de la CABA –Cátedra del Dr. Gustavo Garibaldi– (Facultad de Derecho UBA). Secretaria de Primera Instancia del Ministerio Público de la Defensa de la Ciudad Autónoma de Buenos Aires - Dirección de Jurisprudencia.

Para comenzar, y a los fines de esclarecer qué entiendo por delitos informáticos, tomaré lo que parte de distinguida doctrina clasifica como delitos informáticos *impropios*, es decir, aquellos delitos que utilizan algún medio electrónico o informático para lograr su consumación:

> La doctrina ha clasificado los delitos informáticos según el objeto de protección. Si el "bien jurídico afectado se relaciona con los datos o información automatizada" a la que se accede de modo no autorizado, los llama propios. En cambio, *son impropios aquellos en los que la informática es utilizada como medio para la comisión de un delito distinto de aquel de acceso no autorizado*. La simple lectura de la ley argentina permite advertir que las comunicaciones electrónicas, telecomunicaciones y tecnologías de transmisión de datos son la modalidad prevista de comisión del delito…[1] [el destacado no corresponde al original].

Las modernas tecnologías de comunicación, también llamadas TIC, según Marcos Salt, pueden ser definidas como "un conjunto de tecnologías desarrolladas para gestionar información y enviarla de un lugar a otro. Abarca las tecnologías para almacenar información y recuperarla después, enviar y recibir información de un sitio a otro".[2]

En el año 2008, mediante una modificación a la parte especial del Código Penal realizada a través de la Ley N° 26388 (04/06/08), nuestro país concordó sus tipos penales vinculándolos con las nuevas modalidades de comisión delictiva generadas por las tecnologías de la información y comunicación (TIC) y adaptó su legislación al "Convenio sobre Cibercriminalidad" celebrado en Budapest en 2001. Luego adhirió al mencionado Convenio.

Entre los delitos incorporados, es importante mencionar la tenencia de pornografía infantil con fines de distribución (actualmente modificado), distribución o comercialización de pornografía infantil, el acceso no autorizado a sistemas informáticos, la falsificación o alteración de documentos electrónicos, la producción y distribución de virus y código malicioso, el daño informático y la estafa informática.

Luego, mediante la Ley N° 26904 (BO del 11/12/2013) se sancionó el artículo 131 CP, que prevé el *grooming*.

1. Garibaldi, Gustavo E. L., "Aspectos dogmáticos del *grooming* legislado en Argentina" en *Revista Pensamiento Penal*, 01/06/2015. Disponible en: http://www.pensamientopenal.com.ar/system/files/2015/06/doctrina41215.pdf

2. Salt, Marcos, *Nuevos desafíos de la evidencia digital: Acceso trasfronterizo y técnicas de acceso remoto a datos informáticos*, Buenos Aires, Ed. Ad-Hoc, 2017, p. 11.

En lo que aquí interesa, dentro de los delitos que utilizan un medio electrónico para su comisión, el fuero local (Penal, Contravencional y de Faltas de la Ciudad Autónoma de Buenos Aires) tiene competencia para investigar y juzgar los delitos previstos en el artículo 128 y 131 del Código Penal. Además, a comienzos de 2017, la Fiscalía General de la CABA, mediante el Criterio de Actuación FG N° 01/2017 instruyó a los fiscales a aceptar y defender la competencia en los casos donde se investigue el delito previsto en el artículo 301 *bis* del CP (creado por Ley nacional N° 27346), vinculado al juego sin autorización bajo "cualquier modalidad o sistema de captación de juego".

Como podrá advertirse en los acápites que siguen, este cambio social producido, en parte, por la incorporación de las nuevas tecnologías en nuestra vida cotidiana ha posibilitado, entre otras cosas, registrar, almacenar, buscar y reproducir, con considerable facilidad, imágenes, archivos y conversaciones de personas que, si bien son ventajosos para la investigación de posibles delitos, también pueden llegar a violentar derechos y garantías constitucionales de las personas involucradas. Ello, obviamente, incide de manera notoria en el sistema penal que, si bien viene realizando algunos cambios para acompañar este proceso, aún las deficiencias son muchas, de manera que no solo influyen en la investigación de los denominados delitos informáticos, sino también en el proceso judicial de cualquier delito en el que se utilicen estas tecnologías como instrumentos.

Es por ello que la falta de capacitación de los operadores judiciales, la deficiente regulación procesal respecto de la cuestión probatoria y la falta de criterios unificados acerca de determinados conceptos puntuales, entre otros muchos temas que se desarrollarán a continuación, conllevan que se genere una gran tensión entre la eficacia que debe tener el Estado para investigar estos delitos y las garantías que se deben respetar de todos los ciudadanos que quedan involucrados por la utilización de estas nuevas tecnologías que no se encuentran debidamente reguladas.

Es así que, mediante la exposición de estas problemáticas y, sobre todo, a través del análisis de la jurisprudencia del fuero local, pretendo invitar a los operadores judiciales –en especial, a los integrantes del Ministerio Público de la Defensa– a repensar qué estrategias definir y ver de qué manera plantear determinados cuestionamientos a los fines de defender la legalidad de los procedimientos llevados a cabo

en la investigación de este tipo de delitos y, sobre todo, el respeto a las garantías constitucionales de todos los habitantes.

Problemas específicos de los delitos informáticos

En este acápite mencionaré algunas de las características propias de este tipo de delitos que, como se verá, implican que –necesariamente– se les debe dar un tratamiento específico y diferente al que se le brinda a otros ilícitos ya que, frecuentemente, su investigación resulta mucho más compleja que en otros casos.

Entre estas características, Palazzi[3] resalta, por ejemplo, la magnitud de los daños que pueden ocasionar, la naturaleza global e internacional de esta clase de delitos, la facilidad para cometerlos y las dificultades para la investigación. Este autor indica que, a su vez, ello ha llevado a la necesidad cada vez mayor de cooperación entre las fuerzas de seguridad y el sector privado debido a la necesidad de preservar datos en el tráfico de los proveedores de servicios de internet (ISP), servidores y las empresas de *hosting* y numerosas reconfiguraciones de los esquemas tradicionales con los que se concibe el derecho penal.

Por su lado, para el Dr. Gustavo Aboso[4] los problemas puntuales de los delitos informáticos resumidamente son:

> 1) La determinación de la ley penal aplicable cuando la infracción es cometida en lugares de extraña jurisdicción; 2) la superposición de jurisdicciones penales aptas para castigar esta clase de delitos; 3) la dificultad de individualizar al autor; 4) la participación de personas jurídicas en su comisión; 5) la discontinua anomia que se presenta en los ordenamientos penales frente a estos delitos; 6) la imprecisión de definir el objeto de protección.

Es decir, en su mayoría, se trata de delitos transnacionales, cuyos efectos pueden extenderse por toda la red o se puede dar el caso de delitos que pueden comenzar la ejecución en un país y generar efectos en otros (como la estafa informática, el daño informático, el lavado de activos, la pornografía infantil, etc.).

3. Palazzi, Pablo, "El delito de ofrecimiento y distribución de imágenes relacionadas con la pornografía infantil y de tenencia con fines de distribución", en *Revista de Derecho Penal y Procesal Penal*, Buenos Aires, Abeledo Perrot, 2009.

4. Aboso, Gustavo, "Asociación de Magistrados y Funcionarios de la Justicia Nacional", *Revista Jurídica*, año XV, N° 28, enero-abril 2002, p. 276.

La transnacionalidad supone que las pruebas del ilícito puedan estar tanto en el dispositivo desde donde se cometió el hecho como en los distintos sistemas vulnerados, sean redes, sitios *web* o computadoras.

Otro de los puntos importantes es que, en general, los delitos informáticos son anónimos, ya que Internet permite la posibilidad de crear identidades ficticias (creación de perfiles falsos en una red social) o porque el autor del delito conoce la forma de ocultar su identidad, por ejemplo, a través de la navegación anónima en Internet mediante algún programa especial. Esto trae aparejadas dificultades en torno a determinar la autoría y participación del sujeto activo del delito, ya que muchas veces los dispositivos utilizados para la comisión del delito son de acceso compartido por varias personas.

Además, debido a la gran capacidad de almacenamiento que tienen los dispositivos, un gran problema se presenta con la habilitación legal para intervenir en el ámbito de la intimidad del domicilio, la correspondencia (*e-mails*) y los archivos privados. Ello, ya que el secuestro de elementos de prueba muchas veces excede el objeto de la investigación y se produce una verdadera intromisión en ámbitos protegidos constitucionalmente.

Finalmente, relacionado con lo manifestado en el párrafo anterior, uno de los argumentos que me generan, en lo particular, mayor preocupación, es la fundamentación de la "extrema gravedad" de estos delitos que realizan algunos operadores judiciales como elemento de valoración a la hora de sopesar entre resguardar las garantías constitucionales del imputado y las de los terceros damnificados ante medidas de investigación intrusivas y la necesidad imperiosa del descubrimiento de la verdad. En este sentido, Marcos Salt refiere:

> Una adecuada protección de las garantías fundamentales requiere prestar atención a este argumento de la "gravedad del delito investigado" como elemento de ponderación que limita el ámbito de incidencia de una garantía en un caso concreto. Esta utilización de la idea de proporcionalidad entre el costo de una nulidad probatoria en un caso concreto frente a la afectación del delito concreto que se investiga ha sido esgrimido muchas veces para justificar avances sobre garantías individuales que, posteriormente se terminan extendiendo de manera más general...[5]

5. Salt, Marcos, *op. cit.*, p. 44, nota al pie 51.

Regulación normativa en materia de delitos informáticos. El Código Procesal Penal de la Ciudad Autónoma de Buenos Aires

La evidencia digital no es sólo una cuestión relacionada con los "delitos informáticos" sino un tema fundamental en la prueba de cualquier delito. Es por ello que resulta fundamental analizar si la regulación vigente en materia procesal penal es suficiente y adecuada para permitir primero, la obtención, el análisis y, finalmente, la incorporación legítima de estos elementos de prueba o evidencia informática, electrónica o digital al proceso.

La Ley N° 26388 que incorporó los delitos informáticos a nuestro Código Penal es una ley sustantiva que no fue acompañada por una reforma procesal. Si bien es cierto que esta ley vino a dar cumplimiento (parcial) al Convenio sobre ciberdelincuencia de Budapest, celebrado en el año 2001, lo cierto es que, en realidad, sólo adaptó nuestra legislación en lo que refiere al derecho penal sustantivo, previsto en el Capítulo II, pero no adaptó nuestra legislación a la Sección 2 destinada al "derecho procesal" por este instrumento internacional.

> En igual sentido tampoco se ha dado cumplimiento a la sanción de una legislación que prevea la "conservación rápida de datos informáticos almacenados", conforme lo requerido por el mencionado convenio en su sección 2, Título 2. Así es que resultaría indispensable una legislación nacional que prevea lo prescripto por los siguientes artículos del Convenio sobre la Ciberdelincuencia de Budapest: 1) la conservación rápida de datos informáticos almacenados (art. 16). 2) Conservación y revelación parcial rápidas de los datos relativos al tráfico (art. 17). 3) Orden de presentación (art. 18). 4) Registro y confiscación de datos informáticos almacenados (art. 19). 5) Obtención en tiempo real de datos relativos al tráfico (art. 20). 6) Interceptación de datos relativos al contenido (art. 21).[6]

Es indudable, como vengo sosteniendo, que la evidencia digital tiene características propias que la diferencian de la evidencia física a la que todos los operadores judiciales e, incluso, personal de la prevención están acostumbrados a manejar. Esto, como se advierte, gene-

6. Sueiro, Carlos Christian, *Criminalidad informática. La eficacia político-criminal de la reforma al Código Penal en materia de delitos informáticos*, Buenos Aires, Editorial Ad-Hoc, 2015, pp. 187-188.

ra un desafío y un compromiso de capacitación, reflexión y cambios, tanto legislativos como del modo de actuar ante la aparición de estas nuevas tecnologías en el proceso penal.

Diferencias entre la evidencia física y la evidencia digital

La evidencia digital se puede definir, conforme lo sostiene el FBI, como "datos que han sido procesados electrónicamente y almacenados o transmitidos a través de un medio informático". Este almacenamiento o transmisión puede ser realizado, por ejemplo, en memoria de almacenamiento, memoria RAM o tráfico de red.

Dada esta disímil naturaleza con la prueba física, es obvio que existen numerosas diferencias entre la evidencia informática y la evidencia tradicional. Entre las diferencias más salientes puedo citar: la volatilidad de la prueba informática, la capacidad de duplicación, la facilitación para alterarla, la cantidad de metadatos que posee, además de que el dato informático no es visible para una persona sin conocimientos y formación técnica específica. Otra diferencia es la dificultad en la búsqueda de la información pertinente para el objeto procesal, debido a la cantidad de datos que se pueden almacenar en un dispositivo o en la red.

En este sentido, algunas de las características propias de las evidencias digitales son: su fragilidad, que puede crearse una copia idéntica y que pueden crearse copias no autorizadas sin dejar rastro.

Por otro lado, también merece especial atención todo lo que respecta a la cadena de custodia, que es un registro minucioso del movimiento de la evidencia durante el proceso probatorio y que indica –o debería indicar– con exactitud las actividades realizadas, las personas responsables, el momento y el estado al contacto con la evidencia. Permite asegurar y demostrar la identidad, integridad, preservación y registro de continuidad de la prueba.

Teniendo en cuenta estas características particulares, y al no existir una regulación específica, se plantean múltiples interrogantes, por ejemplo, en torno a lo atinente a la prueba obtenida a través de interceptación de las comunicaciones telefónicas.

La finalidad de la intervención de las comunicaciones (ya sean llamadas, videoconferencias, mensajería instantánea, entre otras) realiza-

das o recibidas por el imputado es la obtención de datos o elementos de prueba para la investigación. Sin embargo, esta potestad se encuentra restringida a los jueces que son los que tienen la facultad de emitir esas órdenes. Dichas medidas deberán estar siempre fundamentadas y se deberá explicitar cuáles serán las condiciones precisas para su ejecución.

Ello, ya que la resolución que ordena una interceptación de comunicaciones, que de por sí significa una restricción o injerencia en el ámbito de un derecho fundamental, debe estar motivada por las constancias y necesidad de la causa y debe ser fundada.

Ahora bien, anterior a ello se debe acordar acerca de cómo debe interpretarse la frase "intervención" de comunicaciones. Respecto de este tópico, en el acápite referido a las resoluciones judiciales comentaré el fallo "Acosta"[7] del Tribunal Superior de Justicia de la Ciudad, que sentó las bases de interpretación acerca de lo que debe entenderse por intervención de comunicaciones y cuáles de los informes solicitados por la fiscalía a las empresas de comunicación son los que necesitan de autorización judicial.

Por otro lado, la problemática que se presenta es que si no existe en la legislación procesal local una regulación específica sobre la recolección, conservación e incorporación de la evidencia informática, ¿cómo debe procederse para resguardar la legalidad del procedimiento?

En virtud de este primer interrogante, una de las soluciones posibles, conforme exponen algunos doctrinarios, y según lo decidido por muchos jueces en casos concretos, es aplicar analógicamente la normativa procesal existente para la prueba física o tradicional.

Sin embargo, entiendo que este intento de solucionar el problema no resulta adecuado ya que, en muchos casos, la aplicación sin más de aquellas normas significa una restricción o vulneración de garantías constitucionales. Porque lo cierto es que la cuestión será determinar si la vulneración a la privacidad que importa la utilización de esta clase de medios probatorios debe primar frente al deber del Estado de perseguir delitos, o si es violatoria de la garantía del *nemo tenetur*, o de la garantía de la privacidad, intimidad, entre otras.

Entonces, ante este cuadro de situación, cabe preguntarse hasta qué punto se debe admitir la aplicación analógica *in malam partem* de

7. "Ministerio Público –Fiscalía de Cámara Norte de la CABA– s/ queja por recurso de inconstitucionalidad denegado en 'Acosta, Cristian s/ infr. art. 128.2, párr. 2°, CP'", Expte. Nº 13576/16, rta. el 04/04/2017.

normas que no han sido incluidas expresamente en la disposición procesal que impone una interpretación restrictiva, pero cuya aplicación (analógica) genera un perjuicio en el imputado.

Así, si lo que se desea es aplicar nuevas tecnologías en el procedimiento penal con el objeto de probar hechos, pero esos medios de prueba aún no han sido regulados, lo que corresponde es una modificación legislativa para prever en la ley procesal penal el modo de adquisición, conservación e incorporación de estos medios probatorios. Incluso, entiendo que esa previsión legal deberá hacerse con una precisión y exhaustividad mayor que la utilizada para los medios de prueba tradicionales, dada la extrema complejidad de las nuevas tecnologías y su altísima capacidad invasiva de la privacidad.

En nuestro país, en general, salvo algunas excepciones, las leyes procesales penales no incluyen mecanismos dedicados de manera exclusiva a la regulación de la investigación de los ciberdelitos, más allá de las normas procesales que autorizan en líneas generales la interceptación de las comunicaciones y el secuestro de correspondencia o papeles privados (art. 231 y ss. del Código Procesal Penal de la Nación; arts. 115 y 117 del Código Procesal Penal de la Ciudad Autónoma de Buenos Aires, entre otros), en los términos previstos por el artículo 18 de la Constitución Nacional.

El Código Procesal Penal de la Ciudad Autónoma de Buenos Aires, en el artículo 113, establece que

> El/la Fiscal, o el/la Juez/a cuando así lo requiera el cumplimiento de las garantías constitucionales en general o respecto de los elementos mencionados en el artículo 13 inciso 8 de la Constitución de la Ciudad Autónoma de Buenos Aires, podrán disponer la requisa y/o el secuestro de las cosas relacionadas con el hecho, o aquellas que puedan servir como medios de prueba.

El mismo artículo contempla expresamente que "Cuando el secuestro fuera de documentos, *equipos de computación u otro soporte informático*, deberá guardarse reserva de su contenido con igual alcance que el previsto para la interceptación de correspondencia y comunicaciones".

En este sentido, la Constitución de la Ciudad de Buenos Aires, en el artículo 13, inciso 8 dispone: "El allanamiento de domicilio, las escuchas telefónicas, el secuestro de papeles y correspondencia *o información personal almacenada*, solo pueden ser ordenados por el juez competente" (el destacado me pertenece).

Es decir,

> … la CCABA agrega a los supuestos contemplados en la Constitución Nacional, las comunicaciones telefónicas, la información personal y el derecho a la privacidad, intimidad y confidencialidad; derechos todos ellos, que han sido entendidos por la CSJN protegidos también por la CN (cf. Entre otros, la sentencia *in re* "Halabi", CSJN- Fallos: 332:111), aun cuando no son mencionados de modo expreso (TSJ CABA, 4/11/14 "Blanco, Diego Alejandro", expte. N° 9978/13, del voto del Dr. Lozano en mayoría).[8]

Sin embargo, a pesar de esta previsión legal, en nuestro fuero local se ha suscitado muchas veces la discusión, a raíz de planteos de nulidad interpuestos por la Defensa, respecto de la falta de autorización judicial en algunas ocasiones, sobre el modo en que las fuerzas de seguridad acceden a la evidencia digital, al procedimiento de almacenado, conservación, a la cadena de custodia o a la nula participación de la defensa en estos procedimientos, donde también se pone en duda su irreproducibilidad.

Continuando con las previsiones legales del Código de Procedimiento Penal de la CABA, merece especial atención la redacción del artículo 117, que textualmente dice:

> Artículo 117. Intervención de comunicaciones. Ante pedido fundamentado del/la Fiscal, el/la Juez/a podrá ordenar, mediante auto, la intervención de comunicaciones del/la imputado/a por cualquier medio, para impedirlas o conocerlas. La intervención de comunicaciones tendrá carácter excepcional y sólo podrá efectuarse por un plazo de treinta (30) días, pudiendo ser renovada sólo una vez por quince (15) días más, expresando los motivos que justifican la extensión del plazo. Rige para los funcionarios encargados de efectuar la intervención el deber de confidencialidad y secreto respecto de la información obtenida por estos medios, excepto respecto de la autoridad que la haya requerido. Quienes incumplan este deber incurrirán en responsabilidad personal. En ningún caso podrá usarse este medio de investigación para eludir el derecho del/la imputado/a de negarse a declarar sin que ello importe presunción en su contra o suplir las declaraciones testimoniales prohibidas por vínculo de parentesco o secreto profesional.

En el fuero local, es el fiscal quien mayormente requiere los informes de llamadas entrantes y salientes de un abonado a las com-

8. De Langhe, Marcela y Ocampo, Martín, *Código Procesal Penal de la Ciudad Autónoma de Buenos Aires. Análisis doctrinal y jurisprudencial*, Buenos Aires, T. 1, 2017, p. 378.

pañías telefónicas, así como los datos de la titularidad de las líneas, sin autorización judicial y sin que ello sea considerado por la jurisprudencia mayoritaria del fuero como violatorio a lo previsto en el artículo 117 CPPCABA, ni al derecho a la intimidad protegido por la Constitución Nacional. De este modo lo han entendido los jueces de la Sala I en "Márquez, Martín Ariel", causa N° 57433-02/10, rta. 30/3/2012, "Pollini, Ricardo Isidoro", causa N° 28760/11, entre otros. Asimismo, en el mismo sentido se expidió la Sala II en "Álvarez, Juan Manuel", causa N° 7707-01/14, rta. 5/11/2015.

En cambio, y compartiendo los fundamentos que, generalmente, introduce la Defensa, se ha expedido el Dr. Delgado, integrante de la Cámara de Apelaciones del fuero:

> Por el contrario se ha resuelto que resulta necesario establecer, en primer lugar, el alcance del significado dado por el legislador a la expresión "interceptaciones telefónicas" y si esta expresión comprende un informe sobre la nómina de llamados recibidos por un teléfono y la indicación del teléfono de procedencia. Una amplia protección al derecho a la intimidad obliga a entender que tanto el contenido de las conversaciones (lo único que, aunque metafóricamente, podría ser apropiado antes de que llegue a destino), como la nómina de llamadas, su procedencia y duración, se encuentran alcanzados por la regla que ampara la privacidad y solo con orden judicial pueden requerirse informes sobre estos datos, en principio, reservados [CAPCF, Sala II, 26/9/12, "Lezcano, Diana Alexandra", causa N° 2955/12, del voto en disidencia del Doctor Delgado].[9]

Asimismo, el artículo 115 del CPPCABA dispone:

> Artículo 115. Interceptación de correspondencia. Prohibición. Urgencia. Siempre que lo considere útil para la comprobación del hecho, ante el pedido fundamentado del/la Fiscal, el/la Juez/a ordenará, mediante auto, la interceptación y el secuestro de la correspondencia postal o telegráfica o de todo otro efecto remitido por el/la imputado/a o destinado a este/a en cualquier soporte, aun cuando sea bajo nombre supuesto. *Los integrantes de la policía y fuerzas de seguridad deberán remitir intacta la correspondencia secuestrada a la autoridad judicial o del Ministerio Público Fiscal competente*. En los casos urgentes, podrán ocurrir a la más inmediata, la que autorizará la apertura si lo creyere oportuno [el destacado me pertenece].

9. Ibídem, p. 379.

Aquí, como lo adelanté, uno de los puntos críticos está en dilucidar qué se entiende por "interceptar", por "correspondencia" o por "comunicación". Será de acuerdo a la interpretación otorgada a estos términos el límite que se le imponga al Estado en la intromisión de las garantías fundamentales de los habitantes.

En esta línea, otro punto para reflexionar debe ser el que prevé el artículo 115 *in fine* del CPPCABA (que en la transcripción anterior destaqué) ya que en la práctica judicial se puede observar que, muchas veces, en ocasión de efectuarse los allanamientos, no sólo se secuestran computadoras sino que, en ocasiones, las fuerzas de seguridad que llevan adelante la medida en ese momento reproducen, abren o indagan el contenido de los elementos secuestrados. De esta manera, a simple vista se puede observar el incumplimiento de la reglamentación procesal referida, en cuanto dispone que "los integrantes de la policía y fuerzas de seguridad deberán remitir intacta la correspondencia secuestrada a la autoridad judicial o del Ministerio Público Fiscal competente".

Como se advierte, la legislación es vaga e insuficiente y no se puede dejar al libre arbitrio de los jueces en el caso a caso un tema tan delicado como el que vengo desarrollando. Por los motivos expuestos, considero que se debe realizar una modificación urgente en las normas procesales que regulan la obtención de evidencias, la incorporación de aquellas como prueba en el debate, la previsión expresa donde conste qué se entiende por comunicación, intervención, entre otros.

Ello, toda vez que no es posible continuar aplicando analógicamente (*in malam partem*) y en perjuicio del imputado, reglamentaciones existentes para la prueba física a la evidencia electrónica.

De continuar así, considero que se está realizando una injerencia en la intimidad de las personas sometidas a este tipo de procesos que no puede permitirse so pretexto de la gravedad de los delitos investigados.

Planteos más frecuentes realizados por la defensa

En este acápite pretendo poner de resalto cuáles son los planteos que con más frecuencia se introducen desde la defensa en casos de tenencia o distribución de pornografía infantil o de *grooming*.

Particularmente, y ante el universo de casos relevados hasta el momento,[10] puedo sostener que, mayormente, los planteos esbozados en torno a los delitos encuadrados como infracción a los artículos 128 y 131 del Código Penal se relacionan con cuestionamientos relativos a:

1. Legalidad de la *noticia criminis*. Pedido de nulidad del informe remitido por National Center for Missing and Exploited Children (NCMEC). Esta solicitud de nulidad se funda en que, para la Defensa, estos informes son una manera de intervenir las comunicaciones, por lo que, necesariamente necesitan de una autorización judicial.
2. Cadena de custodia. Problemática respecto de la legitimidad en la adquisición e incorporación al proceso de las evidencias electrónicas y los resguardos que se le da a la evidencia obtenida, cuestionando la cadena de custodia de estos.
3. Participación de la Defensa en las pericias o "informes" de los dispositivos de almacenamiento secuestrados. El problema legal aparece si lo que se inicia como una búsqueda muchas veces, en la práctica, se transforma en una verdadera pericia en la que no se respetan las normas de procedimiento, entre otras, la participación de la Defensa (conforme, por ejemplo, lo previsto en el artículo 130 del CPPCABA). Una de las soluciones a eso, entre muchas otras, sería que se utilicen técnicas de bloqueo de escritura sobre los medios de almacenamiento o que la búsqueda concreta o pericia se realice en otro momento, con presencia de todas las partes y no en el momento del allanamiento. Entonces, si de esa búsqueda surgen elementos nuevos, en todo caso, la fiscalía podría solicitar un nuevo allanamiento si fuera procedente.
4. Planteos de nulidad por falta de intervención jurisdiccional en los pedidos de informes a Microsoft o compañías telefónicas para solicitar la IP del imputado. Aquí también el fundamento de la nulidad se basa en que la solicitud de estos informes es efectuada por la Fiscalía sin previa autorización judicial.

10. Bases de datos consultadas desde la Dirección de Jurisprudencia del MPD (Juristeca, Información Legal, El Dial, información brindada por las Defensorías de Primera Instancia PCyF).

5. Atipicidad del delito por falta de corroboración del elemento subjetivo del tipo. Así, en las causas investigadas por el delito de *grooming* se ha planteado la atipicidad por falta de demostración de la ultra finalidad que exige el tipo, es decir, "el propósito de cometer cualquier delito contra la integridad sexual de la misma" (refiriéndose al menor). En el delito tipificado en el artículo 128 segundo párrafo (tenencia con claros fines de distribución), planteos por falta de pruebas en cuanto a la demostración de los fines inequívocos de distribución que no se pueden basar, según los planteos de la Defensa, en la cantidad de material con la que contaba el imputado (artículo actualmente modificado por la Ley N° 27436, art. 1 B.O. del 23/04/2018 que ahora pena la mera tenencia).
6. Comienzo de ejecución. En casos de *grooming*, otra de las problemáticas específicas reside en determinar a partir de qué momento habría comienzo de ejecución, ya que si se entiende que tomar contacto con el menor es un acto preparatorio, estaríamos ante una calificación que habilitaría el adelantamiento temporal de punición por parte del Estado.
7. Falta de demostración del principio de lesividad, tanto en el delito tipificado en el artículo 128 como en el previsto en el artículo 131 del CP.
8. Cuestiones referidas a la competencia territorial (transterritorialidad). Las normas procesales vigentes no han previsto expresamente la posibilidad de que los datos informáticos necesarios en el marco de una causa penal estén ubicados físicamente en extraña jurisdicción. Ello aún no se ha regulado en nuestro código procesal ni en la mayoría de los procedimientos del país. Además, se plantean numerosos incidentes de competencia territorial ya que, otro de los temas a tener en cuenta es que, muchas veces, el supuesto delito tiene su comienzo de ejecución en un determinado lugar y continúa perpetrándose en otra jurisdicción, para culminar con sus efectos en un lugar distinto a los anteriores.
9. En la etapa intermedia (audiencia de admisibilidad de prueba): generalmente las defensas se oponen a la incorporación de determinadas evidencias, ya sea porque plantean la nulidad en

la obtención de la misma o porque entienden que la evidencia que la fiscalía pretende incorporar al juicio excede el objeto de investigación, podría generar prejuicio en el juez del debate, entre otras fundamentaciones. Sin embargo, muy pocas veces los jueces realizan un análisis estricto de admisibilidad de la prueba, argumentando que existe la amplitud probatoria.

Entonces, se pone en juego el concepto de la amplitud probatoria o libertad probatoria *versus* el principio de legalidad. Aquí es importante la interpretación que deberá darse al artículo 106 del CPPCABA, que prevé:

> Artículo 106. Amplitud probatoria. Los hechos y las circunstancias de interés para la solución correcta del caso podrán acreditarse por cualquier medio de prueba que no resulte contrario a los principios contemplados en este Código. No regirán las limitaciones establecidas por las leyes civiles respecto de la prueba, con excepción de las relativas al estado civil de las personas.

En este aspecto, deberá tenerse en cuenta que la gran capacidad de almacenamiento de los dispositivos permite generar numerosos documentos digitales. El gran problema surge de la identificación de la evidencia digital adecuada a los fines de la investigación, en un dispositivo o sistema informático que puede almacenar o transportar miles o millones de documentos. Aquí se encuentran en tensión, por un lado, las garantías del sujeto investigado o imputado ya que existe una alta probabilidad de que se encuentre información que no hace al objeto de la investigación y sí al fuero de la intimidad y privacidad, lejano al objeto que determinó la medida. Y, por otro, la responsabilidad del Estado en la investigación de estos delitos.

Muchas veces, las órdenes de allanamiento no describen con precisión el objeto de la búsqueda relacionado con la evidencia digital y emplean, en algunas ocasiones, fórmulas abiertas que rozan o, directamente, conculcan garantías constitucionales y, además, habrá que plantear oposiciones al momento de que la fiscalía pretenda la incorporación en el debate de esos elementos obtenidos.

En este sentido, la idea de "libertad probatoria" choca de manera especial con el principio *nulla coactio sine lege* que determina, en relación

> con el tema que es objeto de la presente investigación, procedimientos probatorios o medios de prueba que impliquen algún grado de injerencia (o la utilización de coerción) en el ámbito de derechos fundamentales reconocidos por la Constitución Nacional o los Pactos Internacionales de Derechos Humanos de jerarquía constitucional (CN, art. 75, inc. 22) deben estar previstos en leyes que, por otra parte, deben cumplimentar los requisitos propios de la reglamentación constitucional que exige que el legislador no altere, sustituya o modifique el principio constitucional que reglamenta [...] todas aquellas actividades del Estado, entre las que se encuentra la actividad probatoria en el marco de los procesos penales, que impliquen una injerencia en los derechos fundamentales de los ciudadanos, tienen como condición de validez una autorización legal previa.[11]

10. En el delito de *grooming* se cuestiona la constitucionalidad del monto de la pena, pues la mayor discusión está centrada en la escala punitiva prevista para este hecho delictivo, ya que, tratándose de un acto preparatorio de otro delito, su pena no debería ser igual o superior a la prevista para el ilícito que se intenta consumar. Respecto de ello, se evidencian cuestionamientos en torno a la escala penal, por considerar que entra en colisión con los principios de culpabilidad, de proporcionalidad de la pena y de razonabilidad de los actos de gobierno, previstos por los artículos 18 y 28 de la Constitución Nacional.

Respuestas jurisdiccionales a los planteos de la defensa en el Fuero Penal, Contravencional y de Faltas (PCYF)

Respecto del planteo de nulidad de la *notitia criminis* o del informe remitido por el National Center for Missing and Exploited Children (NCMEC) por no contar con autorización judicial

Tribunal Superior de Justicia

- Expte. Nº 13576/2016 "Ministerio Público –Fiscalía de Cámara Norte de la CABA– s/ queja por recurso de inconstitucionalidad denegado en 'Acosta, Cristian s/ infr. art. 128.2, párr. 2°, CP'"

11. Salt, Marcos, *op. cit.*, p. 45.

En nuestro fuero local se ha suscitado muchas veces la discusión, a raíz de planteos de nulidad de la Defensa, acerca del pedido de informes solicitado por el MPF respecto de la titularidad de la IP a Microsoft o a las compañías telefónicas. Esta solicitud de nulidad parte de la base de que estos informes son una manera de intervenir las comunicaciones, por lo que necesariamente necesitan de una autorización judicial. Algunos jueces integrantes de la Cámara de Apelaciones lo entendieron de esta manera, haciéndose eco de los planteos postulados por la defensa.

Así, la cuestión ha llegado mediante vía recursiva de la fiscalía al Tribunal Superior de Justicia de la CABA en el fallo "Acosta". Allí, los jueces por mayoría (con el voto en disidencia de la Dra. Alicia Ruiz) han entendido que

> En síntesis, considero que para declarar la nulidad de los informes mencionados, la Cámara efectuó una interpretación de las leyes invocadas en su propia sentencia y de las normas procesales en juego que no resulta razonable pues ninguna de ellas, como se vio, autorizaba a equiparar los informes sobre la titularidad del protocolo de internet (IP) a las "comunicaciones telefónicas", ni el pedido que el fiscal efectuó en ese caso con una "interceptación" de las comunicaciones (Voto del Dr. José Osvaldo Casás).
>
> Corresponde examinar los términos "comunicación" e "interceptación". El objetivo es determinar si las constancias de un registro, esto es, aquello por lo que inquiere el fiscal, constituye una comunicación cuya interceptación sólo puede ser dispuesta por un juez [...] En este marco, la tesis de Cámara no se sostiene. Las constancias del registro por cuyo contenido inquiere el fiscal no suponen una comunicación, de acuerdo a lo que el uso natural del castellano, fijado por la RAE, dispone; mucho menos, una susceptible de interceptación. En efecto, no se está interfiriendo "algo en su camino" o "antes de que llegue a su destino", es decir, no se está interceptando [...] Es cierto que en su gestación pudo haber habido comunicación entre la autoridad del registro y el individuo que registra: uno hizo saber su voluntad de registrarse al otro que lo registró. Pero, ni son estas comunicaciones aquellas por las que se inquirió, ni tampoco son de aquellas a cuyo respecto se espera privacidad. En rigor de verdad, los registros indican justamente lo contrario (Voto del Dr. Luis Francisco Lozano).
>
> En la sentencia que viene cuestionada por la Fiscalía, los jueces de Cámara decretaron –por mayoría– la nulidad de los dos informes mencionados, porque –a su juicio– aquellos debieron ser requeridos por orden judicial. De la misma forma, dispusieron la nulidad del requerimiento de juicio por estar basado en los elementos obtenidos sin control judicial

> (fs. 727) [...] según la Cámara los dos informes requeridos por la División Delitos Tecnológicos de la PFA, en virtud de la orden Fiscal, son una "interceptación de comunicaciones" –en los términos de los arts. 93 del CPPCABA o bien el art. 236 del CPPN– por lo tanto solo podrían ser efectuados por orden judicial. Es por eso que declararon la nulidad. Sin embargo, corresponde revocar la sentencia de Cámara toda vez que el decisorio cuestionado presenta vicios en la fundamentación que impiden considerarlo una decisión válida y, además, se aparta, sin motivo, de aplicar las reglas procesales que gobiernan la actuación del MPF para investigar hechos delictivos (Voto de la Dra. Inés M. Weinberg).
>
> ... En efecto, las "comunicaciones", "papeles", "correspondencia" y la "información personal" a las que se refieren todas estas normas, suponen, en realidad, un ámbito de privacidad o de intimidad que por sus particulares características sólo podrían ser materia de intrusión (es decir, interceptación o secuestro) a través de una orden judicial que autorice dicha intromisión; pero *ese ámbito protegido no comprendería a los "informes" destinados a conocer la titularidad del usuario de un bien o servicio, puesto que tales "informes" no constituyen las comunicaciones ni los mensajes personales a los que dichas normas intentan resguardar, ni conllevan implícita una esfera de reserva que deba ser preservada de esa manera* [el destacado me pertenece] (Voto de la Dra. Ana María Conde).

Cámara de Apelaciones Penal, Contravencional y de Faltas

- Causa N° 12322/2015-0 "NN s/inf. art. 131 CP", resuelta el 23/11/2017, Sala I de la Cámara Penal, Contravencional y de Faltas. Dres. Elizabeth A. Marum, José Saez Capel y Marcelo Pablo Vázquez.

En este caso, la defensa sostuvo que el informe remitido por el National Center for Missing and Exploited Children (NCMEC) en el marco del acuerdo para el Acceso Remoto a CiberTipline celebrado entre la organización de mención y el Ministerio Público Fiscal de CABA (Resolución FG N° 435/2013), había sido obtenido en una clara violación de los derechos constitucionales (art. 18 y 19 CN), observándose una interceptación de datos privados sin la debida autorización judicial. Expresó que el reporte emanado por la organización mencionada importó la apertura de correspondencia protegida en los términos de la Constitución Nacional, encontrándose alcanzado por la regla que ampara la privacidad, debiéndose proceder a la interceptación de los datos y contenido del mismo bajo orden de un juez competente mediante auto fundado.

Al respecto, los jueces de la Sala coincidieron con lo manifestado por el Fiscal de Cámara en cuanto sostuvo que "el reporte que dio origen a las actuaciones no vulnera norma constitucional alguna, en tanto la interceptación de ciertos datos de interés no sólo se encuentra prevista en las políticas de privacidad de la entidad donde se abrió la cuenta, sino que se efectuó en cumplimiento del acuerdo suscripto entre el Ministerio Público Fiscal y el 'NCMEC', a los efectos de cumplir con las obligaciones internacionales asumidas".

- Causa N° 8235/2015, caratulada "NN s/ art. 128 párr. 1 del CP", resuelta el 29/04/2016, Sala III.

Nulidad de la *notitia criminis*

El planteo se centró en que las referidas actuaciones se iniciaron, según lo manifestado por el defensor, en violación a lo establecido en los arts. 18 de la CN, 13 inciso 8 de la CCABA, 115 y 116 del CPPCABA. En ese sentido, entendió que se debió haber formulado un pedido de autorización para intervenir comunicaciones. Que el MPF no debería haber iniciado una investigación a través de una *notitia criminis* obtenida en violación de garantías constitucionales en la medida que se interceptan comunicaciones personales sin una orden judicial pertinente, la cual al día de la fecha no había sido solicitada.

Asimismo, la defensa consideró que dicha apertura y el posterior secuestro de la correspondencia –en cualquier tipo de soporte– debían hacerse en presencia del fiscal y del secretario de la Fiscalía, lo cual no había ocurrido.

Los Magistrados de Cámara entendieron que no se advertía un agravio concreto respecto de la manera en que se había iniciado la presente causa.

Planteo de nulidad del requerimiento por falta de fundamentación en la descripción de la conducta típica

Cámara de Apelaciones Penal, Contravencional y de Faltas

- Causa Nº 16467-00-CC/16 "R., D. s/art. 131 CP –*Grooming*–", resuelta el 10/07/2017 Sala I de la Cámara Penal, Contravencional y de Faltas. Dres. Marcelo Pablo Vázquez y Elizabeth A. Marum.

La defensa cuestionó el requerimiento de elevación a juicio sobre la base de que se había utilizado para describir la conducta imputada el mismo verbo típico establecido en la ley "contactare a una persona menor de edad" y que ello era equivalente a una ausencia de descripción de conductas concretas.

Los jueces de la Sala entendieron, sin embargo, que no se lograba, en el caso, descalificarlo toda vez que, a continuación, la pieza acusatoria efectivamente detallaba los reiterados contactos, es decir, el medio utilizado, el contenido y las circunstancias temporales en las que se habían llevado adelante.

Además, los magistrados agregaron que no se trataba de delitos de sencilla prueba y en la descripción acusatoria no había mucho más que prometer la comprobación de que, a partir del contenido de los contactos y las características del contexto (que sí constituyen elementos objetivos), era posible arribar a la certeza de que existía aquella finalidad, ese deseo de obtener el resultado, más allá de su efectiva materialización.

En conclusión, entendieron que era posible deducir que, más allá de la mayor o menor solidez de la pieza cuestionada, no se advertía que la Defensa técnica se encontrara impedida de resistir la acusación durante la audiencia de juicio.

Los jueces hicieron referencia al bien jurídico tutelado por esta especie de delitos, aduciendo que "puede dejar huellas en la víctima que pueden perdurar para toda la vida, y el servicio de justicia cobra entonces una relevancia significativa para abordar la problemática".

Planteo de la defensa en cuanto se opone al peritaje de los dispositivos secuestrados

Cámara de Apelaciones Penal, Contravencional y de Faltas

- Causa N° 1943/2016-1, "NN s/art. 128 Delitos Atinentes a la Pornografía (producir/publicar imágenes pornogr. c/ menores 18) CP (p/ L 2303)" Sala III, resuelta el 13/7/2016 (Mayoría: Votos de los Dres. Franza y Dra. Paz. Disidencia del Dr. Delgado).

La defensa recurrió la decisión que autorizó el peritaje de los efectos secuestrados en el allanamiento realizado en el domicilio de su defendido y, además, se opuso a determinados puntos de pericia.

Los magistrados, en voto mayoritario, entendieron que la pericia dispuesta sobre los elementos incautados en el domicilio del imputado guardaba una directa vinculación con el objeto de investigación, incluidos los puntos cuestionados por la defensa, razón por la que correspondía rechazar la apelación.

Sostuvieron que, en el caso de autos, la medida reposaba sobre motivos suficientes y concretos que "justificaban el ingreso en ámbitos de privacidad del imputado que suponen las maniobras requeridas, directamente orientadas a la comprobación del hecho y determinar sus alcances".

En este sentido, "la hipótesis de investigación de la fiscalía y la propia naturaleza del delito ventilado avalan, razonablemente, la pretensión de la acusación de pesquisar los distintos dispositivos electrónicos encontrados en el domicilio del principal sospechoso" de haber publicado, en un sitio de Internet, un archivo de video en el que se observaría a dos menores de once (11) años dedicadas a actividades sexuales explícitas con un mayor.

Disidencia del Dr. Delgado

En su voto, el magistrado explicó que la presente causa se había iniciado para determinar si el imputado, de 17 años de edad al momento del hecho, había publicado en Facebook un video donde dos mujeres menores de 18 años de edad se exhibían manteniendo actividades sexuales explícitas con una persona adulta.

Pero, según entendió el camarista, dicho video no se encontraba agregado a la causa, sino que había sido reservado por la fiscalía bajo una clave que debía serle requerida y no lo había sido. Sostuvo que tampoco se había afirmado haberlo peritado para determinar la edad de sus protagonistas. Es decir, no existían constancias que permitieran saber cómo se había determinado la edad de las niñas presuntamente involucradas en actividades sexuales explícitas, ni se sabía si tenían aspecto de ser menores de 18 años de edad, ni el tipo de actividades sexuales explícitas que habrían estado efectuando en dicho video, que no habían sido informadas.

Por ello, concluyó que "el allanamiento efectuado por orden judicial y el secuestro de elementos electrónicos del imputado y de todos sus familiares directos no encontraban sustento alguno en esta causa

y debían ser anulados". Ello, ya que "la mera orden de allanamiento no podía, por sí sola operar como causa suficiente y razonable para fundamentar el secuestro de otros objetos"; salvo cuando, a simple vista o sin que sean tomados mayores recaudos se evidencie con ellos la presunta comisión de un delito distinto. Entendió, asimismo, que igual suerte debía correr la pretensión fiscal de peritar cada dispositivo electrónico allí habido. El procedimiento penal debe iniciarse, necesariamente, ante un delito. Su primer objetivo es acreditar el cuerpo del delito y en esta causa ello no consta. Además, expresó que "la medida practicada y la que se recurre son gravemente intrusivas en la privacidad de las personas. La tranquilidad de la familia del imputado ha sido ya gravemente perturbada y ello no debió suceder sin, previamente, verificar la posible comisión de un delito".

Cámara de Apelaciones Penal, Contravencional y de Faltas

- Causa N° 8235/2015, caratulada "NN s/ art. 128 párr. 1 del CP", resuelta el 29/04/2016, Sala III.

En este caso, fueron dos los imputados (pareja conviviente) por lo que, al existir intereses contrapuestos, designaron a dos defensores oficiales. A continuación, mencionaré algunos de los planteos realizados.

Excepción por atipicidad manifiesta

La Defensora del Sr. G. planteó la excepción de atipicidad, tanto del hecho imputado como distribución, calificado en el artículo 128, 1° párrafo del CP, así como también la atipicidad del hecho imputado como tenencia con fines inequívocos de distribución, calificado en el párrafo segundo del artículo 128 de CP. La atipicidad se planteó no solo por la ausencia del tipo objetivo sino también por la falta del tipo subjetivo del artículo 128 1° párrafo del CP. Ello, toda vez que del reporte informado por Missing Children se podía leer el término *upload* y surgía de este que se habrían subido siete archivos. Que el artículo 128 del CP explicitaba ocho verbos típicos y para poder imputar este delito dentro de ellos, la fiscalía había seleccionado y entendido que el verbo que era aplicable a la figura que le estaba imputando a su defendido era el de *distribuir*. Sin embargo, a entender de la defensora, de la prueba colectada en la causa como del reporte inicial, en ningún momento

se expresaba que se haya distribuido sino que solo nombraba que se habían subido –*upload*– siete imágenes. Que dicho verbo, el de subir, no había sido el elegido por el legislador para que se encuentre configurado ese delito, entonces, la fiscalía tendría que haber explicitado y fundamentado las razones por las cuales, en este caso, el verbo *subir* era idéntico o se aplicaba al verbo *distribuir* que es lo que se le imputaba a su defendido. Que en ningún momento se había explicado cómo se distribuyeron esas imágenes pornográficas, más allá de que las había subido, lo cual hacía difícil ejercer una defensa técnica eficaz, cuando no se sabía de qué manera o a quién se las habría distribuido; como tampoco se sabía hacia cuántos destinatarios fueron. Que todo ello significaba una violación explícita al derecho de poder defenderse.

Por otro lado, *tampoco se encontraba debidamente fundamentado el tipo subjetivo*, ya que este delito solo admitía dolo, o sea, de qué manera la fiscalía podía fundamentar que el Sr. G. había tenido el dolo de distribuir, ya no solo que sabía que tenía ese material sino que subiendo esos archivos G. había tenido el conocimiento y la voluntad de hacerlo para su distribución.

Que con relación a la tenencia, de ninguna manera podía llegar a entenderse que por la gran cantidad de material de dicho estilo y, más allá de las críticas morales que podían hacerse por ello a una persona que poseía en su domicilio esa cantidad de material con pornografía infantil, no podía presumirse que no era para consumo personal. La defensa postuló que si se le imputaba la distribución, esto no podía ser una mera presunción, sino que la fiscalía debía demostrarlo, cuestión que en el caso no había ocurrido.

Los jueces de la Sala entendieron que todas esas cuestiones planteadas eran de hecho y prueba y que deberían ser tratadas durante el debate.

Juzgado de Primera Instancia en lo Penal, Contravencional y de Faltas

- Causa N° 53262-04/11, "Juzgado de Primera Instancia en lo Penal, Contravencional y de Faltas Nro. 20, seguida en orden al delito previsto y reprimido por el artículo 128, 1° párrafo, del Código Penal contra P.D.T.", resuelta el 31/03/2016.

En el presente caso, la imputación formulada por la fiscalía en su alegato de apertura en la audiencia de juicio fue que el imputado había divulgado, facilitado y ofrecido, a través de la red eDonkey2000

utilizando para ello el programa eMule, imágenes y videos donde se representaba a personas menores de dieciocho (18) años de edad dedicadas a actividades sexuales explícitas y representaciones de partes genitales con fines sexuales también de personas menores de dieciocho (18) años de edad.

Los planteos de la defensa fueron:

En cuanto a la *materialidad de los hechos*, señaló que el video mencionado en el Hecho I no fue encontrado en ninguna de las computadoras peritadas. Y que los Hechos II y III no fueron materia de peritaje, puesto que al momento de realizarse la pericia estos no eran objeto del proceso. En cuanto al *aspecto subjetivo*, manifestó que la figura requiere dolo directo, por lo que tienen que ser fehacientemente probados tanto el conocimiento actual y cierto como la voluntad del sujeto, lo que no había sucedido.

Por otro lado, entendió que no podía afirmarse que el delito del artículo 128 1° párrafo se haya consumado y, en ese sentido, solicitó la aplicación del artículo 42 CP referente a la tentativa. Ello, puesto que los *verbos típicos* señalados por el fiscal requieren que las representaciones de menores dedicados a actividades sexuales explícitas hayan llegado a alguien, lo que tampoco se probó. También manifestó que los hechos, tal como fueron relatados por la fiscalía, podrían ser encuadrados en el segundo párrafo del artículo 128 CP.

Respecto de la *atipicidad* planteada por cuanto *no existe* otro que recibiera las imágenes, la jueza entendió que no resultaba relevante para la configuración de la conducta típica que se encuentre individualizado o determinado qué usuarios de eMule descargaron el material de las carpetas del usuario del imputado.

> El tipo penal en cuestión sanciona a quien hace pública una representación con contenido de pornografía infantil, mas nada especifica acerca de que deba un tercero recibir efectivamente dicha representación, ni está intrínseco en los verbos típicos de "facilitar" o "divulgar" que este Tribunal entiende que el imputado llevaba a cabo.

En cuanto al *elemento del tipo objetivo referido a la minoridad del sujeto pasivo* del delito en cuestión, se remitieron al informe efectuado por la Dra. Graciela Diletto, en el que, a partir del material existente en el disco rígido externo, concluyó:

> ... que las imágenes periciadas podrían corresponderse a menores de edad entre 12 y 18 meses algunas de ellas, otras de 6 años y entre los 12 a 14 años de edad, no habiendo alcanzado las figuras adjuntadas el completo desarrollo de sus genitales externos y todas las imágenes que me han aportado podrían obedecer a un patrón de minoridad extrema [...] II.- Que el material exhibido cumple con las características requeridas para clasificarlo como pornografía infantil, según los criterios definidos por la O.N.U.

Nulidad del allanamiento

Cámara de Apelaciones en lo Penal, Contravencional y de Faltas

- Causa N° 8235/15, caratulada "NN s/ art. 128 párr. 1 del CP", resuelta el 29/04/2016, Sala III.

Este planteo de la defensa se basó en que se *procedió* a la apertura de los contenidos de las computadoras, los celulares, los *pendrives* y demás elementos secuestrados, sin la presencia del representante del MPF y del Secretario de la fiscalía. Por ello, la defensa entendió que la nulidad se había producido en el curso del allanamiento, al dejar que el personal policial se dedicara a *escudriñar* todas las computadoras y soportes existentes en el domicilio de su defendida, donde abundaban imágenes e información que no tenían nada que ver con el hecho que se investigaba en autos, que se trataba de cuestiones de la vida familiar e imágenes íntimas de su asistida, las cuales debieron ser analizadas en presencia de la representante del MPF y del secretario a fin de determinar cuáles de dichas imágenes eran útiles para la investigación, para no vulnerar el derecho a la intimidad y a la inviolabilidad de correspondencia y papeles privados de su defendida.

Los jueces entendieron que, en el caso, no se interrumpió ninguna vía de comunicación ni se interceptó ningún tipo de correspondencia, por lo que no le hicieron lugar a la nulidad planteada por la defensa de la Sra. B.

Algunas conclusiones

Una de las primeras conclusiones a las que puedo arribar, en virtud del material consultado, así como de la compulsa de los planteos que vie-

nen desarrollando los defensores oficiales en las causas en las que les corresponde intervenir con relación a delitos informáticos y teniendo en cuenta la jurisprudencia mayoritaria de nuestro fuero, es la necesidad imperiosa de contar con conocimientos técnicos especiales, tanto en los organismos de persecución como en las autoridades judiciales que deben analizar las pruebas, como los integrantes del Ministerio Público. Asimismo, la necesidad de contar con herramientas tecnológicas especiales (*software* de investigación y equipamientos adecuados) además de realizar capacitaciones desde el Ministerio Público de la Defensa.

En este sentido, advierto que se evidencia la necesidad de prever mecanismos procesales especiales para poder hacer frente a los desafíos que genera la obtención de evidencia digital, es decir, instrumentos procesales específicos para los delitos informáticos o los delitos que requieren para su investigación del análisis de evidencia digital.

Hacen falta más herramientas que permitan una mejor investigación en las distintas etapas: en la *adquisición*, la *recolección efectiva del objeto*, en la *preservación* (conservación del objeto, ajustar procedimientos para asegurar la cadena de custodia), en el *análisis y búsqueda del material* y en la presentación que, finalmente, se realiza (informe de resultados obtenidos), así como, fundamentalmente, la *capacitación* de los operadores jurídicos y de los técnicos que integran tanto las fuerzas de seguridad como los Ministerios Públicos.

En el Ministerio Público Fiscal existen fiscalías especializadas en delitos informáticos que se encuentran en cada zona judicial, pero esto no está así organizado en el Ministerio Público de la Defensa, como tampoco existen juzgados especializados. Entonces, si tomamos en cuenta lo que vengo exponiendo y lo plasmado en la jurisprudencia local relevada, donde se advierte que la mayoría de los planteos introducidos por la defensa –sobre todo en la etapa preparatoria– son rechazados o diferidos para ser tratados en la etapa de debate por considerarlos cuestiones de hecho y prueba, deviene imperiosa una reflexión acerca de cómo abordar estas problemáticas.

Es así que, hasta tanto se modifiquen las normas procesales locales que regulan el tratamiento de la evidencia digital, será necesario, entre otras cosas, realizar una actividad probatoria desde el MPD más proactiva, solicitando, de ser necesario, el auxilio judicial, por ejemplo, a la hora de peticionar ciertos informes. Además, una mayor capaci-

tación en la temática específica y en técnicas de litigación permitirá discutir y oponer, con mayor precisión, fundamentos y persuasión a la incorporación de determinadas evidencias para evitar que se incorporen a la etapa de debate.

En definitiva, como quedó plasmado en el presente artículo, en la investigación de los delitos informáticos, con fundamento en la *gravedad*, el *repudio moral* y la *propagación* o *masificación* a través de las redes que muchas veces generan, se visibiliza aún más lo que Alberto Binder denomina *antinomia fundamental*, ya que

> ... en la base (fundamentos) de todas las instituciones procesales se encuentra esta contraposición y las normas procesales deben ser vistas, o como herramientas de política criminal o como parte del sistema de garantías, es decir, como herramientas de protección del ciudadano, en este caso, imputado de un delito. En numerosas ocasiones, una misma norma contiene ambas herramientas. No obstante ello, no desaparece la tensión y ella se manifiesta en la interpretación que hagamos de esa misma norma.

Para finalizar, quiero destacar que, a pesar de las numerosas dificultades planteadas, se evidencia un serio compromiso por parte de todos los operadores del sistema judicial que alienta a seguir trabajando en esta área. Pero, específicamente a los integrantes del Ministerio Público de la Defensa, nos interpela el desafío constante de mantener y hacerle frente a esa tensión existente entre la fuerza que impulsa el poder punitivo –que busca que no exista impunidad– y la defensa permanente que debemos realizar de las garantías fundamentales de todos los individuos.

Bibliografía consultada

ABOSO, Gustavo, "La problemática de los denominados delitos informáticos", *Revista de la Asociación de Magistrados y Funcionarios de la Justicia Nacional*, Año XV, N° 28, enero-abril 2002.

_____, "La nueva regulación de los llamados 'delitos informáticos' en el Código Penal Argentino. Un estudio comparado", en *Revista de Derecho Penal, Imputación, causalidad y ciencia. Doctrina. Jurisprudencia*, Ed. Rubinzal-Culzoni, 2010-1.

BINDER, Alberto, *Derecho Procesal Penal. Hermenéutica del proceso penal*, Buenos Aires, Ed. Ad-Hoc, T. I, 2013.

DE LANGHE, Marcela; OCAMPO, Martín, *Código Procesal Penal de la Ciudad Autónoma de Buenos Aires. Análisis doctrinal y jurisprudencial*, Buenos Aires, T. 1, 2017.

GARIBALDI, Gustavo, "Aspectos dogmáticos del *grooming* legislado en Argentina" en *Revista Pensamiento Penal*, 01/06/2015. Disponible en: http://www.pensamientopenal.com.ar/system/files/2015/06/doctrina41215.pdf

GÓMEZ, Leopoldo S. M., *El delito de pornografía infantil. Análisis dogmático. Aspectos procesales para la investigación penal. Guías y documentos internacionales*, Buenos Aires, Ed. Ad-Hoc, 2012.

PALAZZI, Pablo, "El delito de ofrecimiento y distribución de imágenes relacionadas con la pornografía infantil y de tenencia con fines de distribución", en *Revista de Derecho Penal y Procesal Penal*, Buenos Aires, Abeledo Perrot, 2009.

PÉREZ BARBERÁ, Gabriel, "Nuevas tecnologías y libertad probatoria en el proceso penal", *Revista Nueva Doctrina Penal*, 2009/A.

SALT, Marcos, *Nuevos desafíos de la evidencia digital: Acceso trasfronterizo y técnicas de acceso remoto a datos informáticos*, Buenos Aires, Ed. Ad-Hoc, 2017.

SUEIRO, Carlos Christian, *Criminalidad informática. La eficacia político-criminal de la reforma al Código Penal en materia de delitos informáticos*, Buenos Aires, Editorial Ad-Hoc, 2015.

TOMEO, Fernando, *Redes Sociales y tecnologías 2.0*, Buenos Aires, Editorial Astrea, 2013.

Grooming: el desafío para cuidar a los más chicos

ONG Argentina Cibersegura*

Introducción

Todos sabemos las múltiples ventajas que supone Internet, sobre todo para quienes la mayor parte del tiempo la pasamos conectados intercambiando información en diferentes dispositivos. Sin embargo, de la misma forma en la que encontramos beneficios, como pasa en todos los escenarios donde tiene participación el ser humano, también se presentan peligros.

Particularmente, el punto de partida para entender los problemas a los que se enfrentan los menores en Internet, sin duda, es entender que lo que sucede en ese mundo digital se encuentra estrechamente relacionado con las acciones y todo lo que ocurre en el mundo físico. De esta manera la concepción de la realidad debe considerar tanto lo que pasa en el mundo físico de la persona como también todo lo que ocurre en su mundo digital.

El desconocimiento que a veces se hace de estas dos dimensiones como conformadoras del mundo real de cualquier persona genera que se potencien los riesgos y peligros a los cuales puede verse enfrentado particularmente un menor. De hecho, es importante reconocer que las conductas y acciones en redes sociales u otros servicios de Internet que conforman el mundo digital van a tener repercusiones en ambos contextos y como tales pueden afectar sus interacciones tanto físicas como digitales.

No hay que perder de vista que estos mismos medios del mundo digital son utilizados por los cibercriminales para cometer delitos que en ocasiones resultan complejos de imputar, y de ahí la importancia de trabajar sobre la prevención ya que una vez que se materialice el delito la reparación se hace compleja y el daño muchas veces irreversible.

* Organización sin fines de lucro que trabaja para crear un espacio digital seguro a través de actividades de concientización y educación destinadas a distintos públicos de interés.

Grooming: los más chicos expuestos en el mundo digital

Bajo este término se engloban todas las estrategias que realiza un adulto, en este contexto denominado *groomer*, para ganar la confianza de un niño, niña o adolescente, a través de Internet, con el propósito de abusarlo o explotarlo sexualmente. Un adulto es quien siempre ejerce el *grooming*.

De acuerdo a un informe publicado por la OEA,[1] existen dos tipos de *grooming*: el primero es cuando no existe la fase previa de relación y generación de confianza pero el acosador logra obtener fotos o videos sexuales del menor para extorsionarlo. El segundo es cuando existe una fase previa donde el *groomer* busca generar confianza, logrando que los menores entreguen material sexual por sí mismos para volverlo objeto de chantaje. Suele hacerse pasar por un menor, manipular a través de los gustos y preferencias de la víctima y utilizar el tiempo para fortalecer el vínculo. En este segundo escenario es donde se hace más factible que la relación en el mundo digital pase a encuentros en el mundo físico.

Dadas las características que tiene este delito, la educación en temas de seguridad es fundamental para evitar que los más chicos se vean afectados; incluso la concientización debe ser el punto de partida para no caer en muchas de las amenazas informáticas de la actualidad, o en su defecto, que sus consecuencias sean las mínimas aceptables; conocer los riesgos y la manera en que operan las amenazas resulta importante para minimizar sus consecuencias.

Entendiendo el funcionamiento del delito

A menudo los cibercriminales logran su propósito aprovechándose de la inocencia de los niños y niñas, además de que suelen emplear técnicas para engañarlos a través de conductas sociales, lo que se denomina "ingeniería social". Es decir, se valen de la manipulación psicológica y de la persuasión para que voluntariamente la víctima brinde información o realice algún acto que la ponga en riesgo.

1. Disponible en: http://www.iin.oea.org/pdf-iin/2016/publicaciones/InfRegional-ESP008-WEB.pdf

Por ejemplo, el *groomer* puede seducir al menor por medio de la atención o el afecto, al escuchar sus problemas e incluso haciéndole regalos, luego de que lo ha contactado a través de un medio digital. Posteriormente, trata de reducir la inhibición incorporando gradualmente contenido sexual a sus conversaciones o mostrándole material sexual explícito, en busca de un contacto cara a cara.

Las consecuencias del *grooming* pueden variar dependiendo de las condiciones del niño o niña afectado por el delincuente. En una primera instancia, uno de los daños en el menor puede estar relacionado con sufrir afectaciones psicológicas debido a la manipulación o control que pueda ejercer el adulto, y el daño se puede extender si el *groomer* logra obtener fotografías o videos de contenido sexual del menor, o presentarse casos más graves como trata o explotación infantil. Y quizá lo peor puede darse en caso de que se concrete un encuentro, donde las consecuencias podrían ser de carácter físico, pudiendo llegar incluso al abuso sexual.

Dominar el uso de la tecnología no es sinónimo de seguridad

Como ya mencionamos, la educación en temas de seguridad es fundamental para evitar muchas de las amenazas informáticas de la actualidad. Esto es aún más evidente ya que en ocasiones los padres, las madres o en general los adultos que están alrededor de los más chicos no se sienten involucrados en el cuidado de los menores cuando utilizan computadoras, teléfonos inteligentes o tabletas. Desafortunadamente, con la concepción de que los menores conocen más de tecnología que su padre o madre no suele existir un involucramiento activo y aunque puede ser cierto que los menores tengan dominio de la tecnología, la inocencia juega en contra de su seguridad.

Por ello, aunque los menores se desenvuelven con mayor facilidad en el uso de la tecnología, somos los adultos que estamos a su cargo quienes contamos con la experiencia sobre los peligros a los cuales pueden enfrentarse. Así, se vuelve importante no confundir el dominio técnico de la tecnología que podamos tener como adultos con la capacidad de cuidado.

Es así como la educación y concientización en temas de seguridad no solo debe estar enfocada en los menores, sino que los adultos responsables también tenemos la tarea de conocer los riesgos de seguridad, la manera de evitarlos y posteriormente proteger a los niñas, niños y adolescentes.

Privacidad: una arista poco analizada

Los últimos meses han sido bastante polémicos para las grandes empresas que están a cargo de manejar volúmenes inmensos de información de usuarios. Me refiero puntualmente a las redes sociales, ya que la privacidad recobró su papel protagónico en las discusiones de ciberseguridad y volvió a estar en el ojo de la tormenta. Precisamente una publicación a cargo del ICSI[2] (International Computer Science Institute) pone en evidencia la necesidad de considerar los controles de privacidad que deberían tener las aplicaciones destinadas al uso por parte de menores de edad.

El estudio en cuestión analizó más de cinco mil aplicaciones destinadas al uso por parte de niños y público familiar, disponibles en repositorios oficiales entre noviembre de 2016 y marzo de 2018. Una vez analizadas las aplicaciones se pudo determinar que el 57% podría violar la ley COPPA[3] (Children's Online Privacy Protection Act) que regula la recolección de datos de menores de 13 años en territorio estadounidense.

Vale la pena resaltar que estas violaciones incluyen la recolección de información de contacto y geolocalización del menor, compartir datos con terceros contradiciendo los términos de servicio estipulados e incluso información que permitiría el análisis de patrones de comportamiento. Además del uso de métodos inseguros para transferir información en línea y la configuración de forma errónea de la integración en Facebook para menores de 13 años.

En el caso de Latinoamérica ni siquiera existen leyes análogas que regulen la privacidad de los más chicos al momento de usar apli-

2. Disponible en: https://www.nbcnews.com/tech/tech-news/thousands-android-apps-improperly-tracking-kids-data-says-study-n866711

3. Disponible en: https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions

caciones; y dado el estado de madurez de muchos temas de ciberseguridad quizá este sea un tema que aún demore en ser considerado en países de la región.

En muchos casos se da por sentado que la gratuidad en Internet es una ilusión. De hecho, es claro que las plataformas que ofrecen sus servicios sin costo aprovechan nuestros datos para dar valor a su negocio, en parte, basándose en el conocimiento adquirido del comportamiento para luego ofrecer publicidad u otros servicios que podrían resultar de interés con una mayor tasa de efectividad.

Este modelo de operación se traslada a la mayor parte de las aplicaciones disponibles para dispositivos móviles y que suelen utilizar uno o varios servicios de publicidad de terceros para generar ingresos económicos. El problema para la privacidad en este modelo es que en muchos casos no se presta atención al control y seguridad de los datos que se están recolectando. Por lo tanto, cuando se trata de aplicaciones utilizadas principalmente por menores la pregunta no puede hacerse esperar: ¿qué pasaría si los datos de menores llegan a individuos pertenecientes a redes de pedofilia o *grooming*?

Hay que considerar que es mucha la información recolectada: pasatiempos, gustos, patrones de conducta, geolocalización, número y correo electrónico, lista de amigos, entre mucha información adicional. Es necesario regular esta recolección de información y su respectiva protección ya que una fuga de datos puede facilitar significativamente la tarea de un *groomer* a la hora de contactar y ganar la confianza de sus víctimas.

Y al paso acelerado que aparecen dispositivos conectados recolectando información sensible, la superficie de ataque que podría usar un *groomer* se expande. Ya no se puede pensar únicamente en las aplicaciones de dispositivos móviles destinadas a público infantil; es necesario considerar juguetes inteligentes y en general toda la gama de dispositivos de IoT (*Internet of things*) que puedan exponer información sensible de miles de niños y niñas, incluyendo grabaciones y fotografías.

La necesidad de exigir el especial cuidado de la privacidad de los más chicos en Internet es un debate que deberemos enfrentar como sociedad mientras se sigue avanzando en la maduración de las leyes de ciberdelitos que ayuden a enfrentar los peligros en el mundo digital, considerando el *grooming* como uno de los peores.

Anonimato: ¿diversión o riesgo para los más chicos?

Las redes sociales han ido evolucionando desde su aparición, y la facilidad para dar cierto nivel de anonimato no es algo nuevo, de hecho es una de sus principales características; pero últimamente los más jóvenes se han volcado a aquellas cuyo eje principal es el anonimato. Partiendo del hecho de que las redes sociales, como cualquier otra tecnología, no se puede catalogar como algo malo nos debemos centrar en considerar el uso que se hace de estas y los problemas que pueden surgir cuando como adultos se ignora su existencia y las posibilidades que tienen los menores en ellas.

La oferta de redes sociales en sentido tradicional va cambiando todo el tiempo. Facebook es una de las antiguas, con más de 10 años, y ha ido reinventándose y agregando nuevas funcionalidades. En el camino han aparecido otras como Instagram o Snapchat, que gozan de gran popularidad entre los más jóvenes. Pero, al mismo tiempo, otras opciones como ASK, Voxed y aplicaciones como Whisper también se han ido popularizando. En ellas la premisa es interactuar con otros usuarios sin exponer la identidad, el sitio donde estás o cualquier otro tipo de dato individual. Y nos quedaríamos cortos si tratáramos de describir más redes con sus características, ya que posiblemente al momento en que se esté leyendo este texto el panorama haya cambiado en gran medida.

Pero sin lugar a dudas los más chicos han encontrado en la posibilidad de interactuar con otras personas de manera totalmente anónima una característica interesante. Y la realidad es que se abre la posibilidad para encontrar desde comentarios triviales sobre el estado del clima hasta temas que pueden incluir alguna confesión sobre el estado de ánimo, la búsqueda de un consejo o publicaciones con contenido sexual.

Y todo esto nos lleva indefectiblemente a que este intercambio de información sin mayor control deje a los menores expuestos a contenidos que quizá no sean los más apropiados. Se incrementa la posibilidad de propagación de mentiras, rumores o información falsa. Y si bien esto pasa a nivel generalizado con la gran cantidad de información que se puede consumir desde Internet, en estas redes de total anonimato se acentúa al permitir la interacción directa entre usuarios.

De esta manera aumenta la probabilidad de que ocurran estas situaciones, incluso si se trata de influenciar el pensamiento de los más

chicos con respecto a temas de su sexualidad o pensamientos acerca de su cotidianidad. Lo cual nos deja nuevamente ante un panorama propicio para la ocurrencia del *grooming*.

La seguridad de menores en Internet debe ser un esfuerzo compartido

Los esfuerzos para hacer de Internet un espacio cada vez más seguro para niñas, niños y adolescentes requiere de una concepción integral y en la cual se involucren los diferentes actores de la sociedad civil. Es así como desde la parte gubernamental se necesita el desarrollo y mejora de los marcos normativos a la par de la creación de políticas públicas que fomenten la cultura de la ciberseguridad.

Del sector privado es imperiosa la necesidad de que considere la seguridad y la privacidad desde el diseño de sus productos y aplicaciones. Además, debe darse una contribución más fuerte reflejada en el desarrollo de tecnología especializada en proteger a los menores.

Y por supuesto, sobre el resto de la sociedad recae la responsabilidad de la educación en materia de amenazas informáticas. No se debe dejar de lado la importante tarea que como adultos tenemos en el desarrollo seguro de habilidades de los menores en Internet. Como ya lo mencioné, el desconocimiento de la tecnología no inhibe la capacidad de cuidado de los adultos, sino que implica una mayor responsabilidad y esfuerzo para mantenerse actualizados.

Ante este escenario, ¿cómo proteger a los menores?

Pensar en privar a los menores del uso de Internet en busca de evitar riesgos como el *grooming* es una medida drástica e inútil, ya que de manera paralela se les niega el acceso a un conjunto de recursos de gran utilidad como la vasta información, conocimiento o entretenimiento.

En este sentido, evitar que los menores utilicen los medios digitales no es posible, considerando además que estos forman parte de sus vidas. Por el contrario, el enfoque debe estar en el uso controlado y seguro de Internet.

No se debe perder de vista que los niños y niñas de hoy son "nativos digitales", ya que desde muy pequeños tienen acceso a todo tipo de dispositivos y comienzan a interactuar con la tecnología de manera natural.

Sus vidas transcurren por Internet y las redes sociales no son un fin, sino un medio para socializar con sus amigos y compañeros, por lo que es importante saber sobre sus vidas en el mundo digital tanto como en el mundo físico.

Hay por lo menos cinco conductas que pueden facilitar la tarea de mantener protegidos a los más chicos en el mundo digital, para que sigan disfrutando de la tecnología de manera segura.

- La tecnología como medio para cerrar brechas. Ya mencioné lo erróneo que es creer que no es necesario hablar con los chicos de temas relacionados con la seguridad en línea, asumiendo que saben más de tecnología.

  Si bien es cierto que seguramente saben cómo manejar cualquier dispositivo, cómo compartir contenido en cualquier red social o cómo configurar una aplicación en minutos, también es verdad que les es más difícil reconocer cuando pueden estar frente a un caso de *grooming*. Como adultos, en cambio, podemos reconocer y entender los peligros a los que se expone en estas mismas situaciones.

  Así que si hay aplicaciones que el adulto nunca utilizó, nuevas modas que no entiende o todo un mundo digital que le parece completamente extraño, no hay nada mejor que animarse a explorarlo y aprender a usar nuevas herramientas junto a los más chicos. Si no se sabe qué hacer con un nuevo celular, sentarse junto a ellos para que nos muestren algunas de las aplicaciones que utilizan para divertirse. Compartir estos momentos es clave para acompañar a los chicos en el mundo digital, y mientras ellos nos enseñan cómo usar la tecnología, seguramente podremos identificar los riesgos y explicarles a ellos a qué peligros se exponen y cómo cuidarse.
- Reglas claras y un compromiso compartido. Establecer reglas claras es la clave para acordar un uso responsable de la tecnología. Dejar en claro cuestiones como dónde y en qué momentos se pueden utilizar los dispositivos; crear la conciencia de no responder mensajes de desconocidos, no descargar mate-

rial indebido o no acceder a contenido restringido a mayores de edad son algunas de las cosas que vale la pena aclarar.
Debemos ser los adultos quienes expliquemos cuáles son los riesgos que existen y por qué estas normas ayudan a que ellos estén protegidos. No se trata solamente de prohibir o restringir una actividad, sino de que entiendan la razón por la cual deben ser cuidadosos.
Y como el compromiso debe ser recíproco, también va a ser importante como adultos respetar su privacidad y ofrecerles un espacio de diálogo donde ellos puedan plantear sus problemas e inquietudes, con el objetivo de generar un vínculo de confianza con ellos.

- El ejemplo como base de la educación. Para dejarlo en los términos más sencillos posibles, no hacer lo que no queremos que hagan los niños y niñas que están a nuestro alrededor y sobre los que tenemos alguna influencia. Muchos padres se preocupan por la privacidad de sus hijos en línea, por las fotos que suben a una red o la cantidad de amigos con los que interactúan diariamente, pero luego son ellos mismos los que comparten públicamente fotografías de las vacaciones o eventos familiares, no despegan la vista del celular o descargan aplicaciones fraudulentas o material ilegítimo.
- El mundo físico como fuente de analogías. Los ejemplos puede ser la mejor manera de ilustrar una afirmación y generar una idea más clara. En el caso del mundo digital, resulta mucho más sencillo para los chicos poder dimensionar un peligro si se compara con una situación análoga en el mundo físico. Así como nos enseñan que no debemos hablar con extraños en la plaza o en la calle, en Internet debería considerarse de la misma manera a aquellos que no conocemos en el mundo físico, ya que no tenemos forma de verificar quién está realmente detrás de la pantalla y por lo tanto se deben extremar las medidas de precaución.
- El razonamiento inductivo hacia los más chicos. Tratar de imponer una idea a los más chicos es iniciar una batalla que ya está perdida. En cambio, se puede inducirlos a que piensen en los riesgos a los cuales pueden verse enfrentados. Pensar en algunas preguntas disparadoras puede facilitar el

diálogo y abrir un canal de comunicación fluido. Por ejemplo, en lugar de decirle que cierre sus perfiles y los haga privados, quizá sea más conveniente preguntarle si revisó las configuraciones de privacidad, y si sabe quién puede ver todo lo que sube. Eso sí, cualquier pregunta siempre debe hacerse desde una postura de interés y no de control y restricción.

Incorporando la tecnología como una ayuda más para los padres

A esta altura es claro que la mejor forma de lograr que los niños hagan un uso adecuado de la tecnología y eviten ser víctimas de cualquier amenaza es entablar una relación de confianza de tal forma que exista un diálogo permanente que permita conocer el uso que se les da a las aplicaciones y que le permita al menor empoderarse en el manejo de la tecnología.

Adicionalmente a las recomendaciones anteriores, en el mercado existen herramientas de control parental que pueden ayudar por ejemplo a los padres, sin necesidad de invadir la intimidad de los más chicos.

Las herramientas de control parental permiten regular o limitar el contenido al que un menor puede acceder en la computadora, dispositivo móvil, consola de juegos o en Internet, a través de los sitios *web* que se visitan.

El control de las actividades que los niños y niñas hacen en Internet se logra a través de reglas y filtros que evitan el acceso a contenido inapropiado para su edad: ofrecen posibilidad de filtrar contenido que puede estar relacionado con palabras soeces, pornografía, juegos para adultos, servicios que impliquen gastos de dinero, publicidad no deseada, redes sociales para adultos, o en general lo que los padres consideren inadecuado.

El uso de este tipo de herramientas va a ser fundamental para mantener la seguridad de los más chicos. Pero se debe tener cuidado de no utilizarlas para espiar las actividades que realizan los menores, ya que lo más importante es que siempre exista una relación de confianza y no perder de vista que ninguna tecnología va a garantizar total efectividad sin un diálogo fluido con los menores.

Si bien la incorporación de estas herramientas tecnológicas puede ser de gran ayuda en los primeros años en que los menores empiezan a interactuar con la tecnología, a medida que crecen va a ser más importante el empoderamiento para hacer un uso responsable de la misma. Cuando son más pequeños, el uso del *software* de control parental puede ser mayor sin causar mayores problemas, y puede ayudar hasta que los menores comprendan e internalicen las razones detrás de las reglas.

El reto es encontrar el equilibrio entre darles a las niñas y niños las herramientas para que se conviertan en adultos independientes y pasar el tiempo suficiente con ellos para que se sientan protegidos.

Ser padres de una generación conectada

Ya sea que estemos frente a niños pequeños o adolescentes, es bueno recordar que nuestro trabajo es prepararlos para su independencia. Hay que considerar que ellos nunca tuvieron que esperar para escuchar una noticia en la radio o leerla en el periódico un día después de que ocurriera.

Las nuevas generaciones son las primeras de su tipo; generaciones que siempre van a estar conectadas. Para ellos interactuar en Internet es tan normal como caminar o leer. Viven en tiempo real todo el tiempo. Es más normal enviarle un mensaje instantáneo a alguien que llamarlo y hablar, lo que sugiere que llamar te hace parecer viejo o anticuado.

Pero por más "viejos" que seamos, tenemos que estar allí para guiarlos y educarlos para que sean responsables, se comporten de manera adecuada y se cuiden.

Es verdad que estuvimos hablando de los aspectos negativos y riesgos de interactuar en el mundo digital, pero concentrémonos por un momento en lo positivo y en cuán maravilloso es Internet. Pensemos en las aplicaciones interactivas que se usan para aprender y leer, en las posibilidades que brindan las aplicaciones para ver hechos históricos en tours a 360 grados, en vez de ver fotos en un libro. En un mundo en el que podemos comunicarnos en tiempo real sin importar dónde estemos y sin depender de una cabina telefónica o cables, hay muy pocos límites.

Pero controlar ese balance entre las posibilidades casi infinitas de actividades e interacciones y la facilidad para ser víctima de

algunos peligros puede ser tarea difícil, especialmente cuando las niñas y niños conectados solo conocen una vida en línea, y esta es la forma "normal" de comunicarse. Es importante que entiendan que usar dispositivos o mirar una pantalla es un privilegio y deben considerar y conocer cómo protegerse.

Al pensar las posibilidades que tienen los más chicos para estar conectados, una de las primeras cosas para hacer es pasear por la casa y contar el número de dispositivos que están conectados. Muchos pueden olvidar que las consolas de videojuegos y algunos juguetes ahora también entran en esa categoría, por lo que simplemente apagar un teléfono no cumpliría con el objetivo de alcanzar un equilibrio, ya que el niño usaría otro equipo con acceso a Internet.

A medida que la tecnología evolucione, la capacidad de contener o controlar la cantidad de tiempo conectados sin dudas bajará. La Internet de las Cosas (IoT) promete conectar nuestras casas, autos y ciudades. La posibilidad de automatizar y ser informados sobre prácticamente cualquier cosa que hacemos ya no es ciencia ficción, sino una realidad cercana.

Entender lo que hacen los más chicos mientras están conectados es de importancia crítica. Ya sea usando *software* de control parental, monitoreando el tráfico en el *router* o sólo permitiendo el acceso desde áreas comunes en las que se pueda echar un vistazo, se podrá abrir la conversación sobre uso y comportamiento apropiado de la tecnología.

Una táctica útil para garantizar que los más chicos van a estar seguros es entender la funcionalidad de las *apps* que usan. Escuchar cómo les cuentan a sus amigos sobre lo que hacen. Hablar con ellos para saber más y luego descargarlas para ver cómo son. Si bien seguramente no estén diseñadas para adultos, tener este conocimiento extra sobre cuán adictivas pueden ser, qué contenido muestran, con quién permiten conectarse o cómo funcionan permite continuar el diálogo sobre estar protegido y pasar menos tiempo en el dispositivo.

El diálogo abierto y continuo sobre actividad en línea hará que el adulto sea la persona a la que los niños acudan cuando tengan preguntas o preocupaciones. Si sólo se les habla de los riesgos, es poco probable que compartan su experiencia o busquen consejos.

Internet, un espacio comunicacional y de construcción de diálogo intergeneracional

ONG Faro Digital*

Introducción

En los últimos años las tecnologías digitales provocaron un sinfín de cambios en la vida cotidiana. Su impacto puede verse en la economía, la política, la cultura y la vida social. En efecto, prácticamente no quedan espacios o acciones que puedan escindirse de la influencia de lo digital. El objetivo de este capítulo es generar un canal de reflexión que permita abstraerse de la dinámica y vorágine actual, para así construir una mirada analítica y crítica respecto de los vínculos, relaciones y formas de comunicarse entre las personas, en el contexto de un mundo digital y conectado.

"Kids Online", un estudio realizado por Unicef Argentina en 2016, muestra que ocho de cada diez jóvenes de nuestro país sufrieron alguna experiencia negativa en Internet pero que únicamente tres de cada diez dialogan con sus adultos de confianza respecto de problemáticas o tensiones digitales. Estos datos revelan la distancia existente entre las problemáticas que atraviesan la vida de los niñas, niños y adolescentes y la comunicación con los adultos, y sobre todo la necesidad de revertir estos indicadores desde el diálogo y la comunicación.

El punto de partida del análisis deviene de la brecha generacional e informativa que han generado las nuevas tecnologías en la sociedad. Por un lado, existen sujetos adultos que han pasado gran parte de sus vidas sin utilizar las tecnologías de la información y comunicación (TIC). Y por el otro, jóvenes que han nacido en un mundo mediado por Internet. Esta diferencia genera diferentes formas de

* Organización de la sociedad civil que busca fomentar un uso crítico y reflexivo de las tecnologías digitales. Mediante talleres, campañas e investigaciones, se trabaja en la construcción de ciudadanía en el mundo digital.

aprehensión de lo digital. Quien nace rodeado por espacios digitales no requiere de entrenamiento formal para comprender su uso; sus características y formas se naturalizan y se perciben como parte de un escenario cotidiano y natural. En cambio, quienes debieron aprender sistemáticamente el funcionamiento de Internet y sus diversos programas, construyeron un aprendizaje formal y estructurado. Es sin dudas evidente que las diversas formas de incorporación de lo digital generan a su vez diferentes usos y formas de relacionarse con la *web*. Es por ello que surge la necesidad de construir puentes entre estas generaciones, para poder garantizar la convivencia social.

Internet, redes sociales, servicios de mensajería instantánea, aplicaciones y videojuegos surgen como espacios sociales en donde las nuevas generaciones se relacionan con sus pares. A edades cada vez más tempranas, niñas, niños y adolescentes comienzan no solo a utilizar los servicios digitales, sino también a vincularse con los otros mediante esas plataformas. Esta situación divide las aguas entre quienes no están a favor de estos profundos cambios y quienes consideran de manera positiva las nuevas dinámicas socio-digitales.

Surge como fundamental entonces la construcción de una mirada pragmática que pueda reconocer las prácticas, usos y dinámicas de la vida socio-digital intentando lograr así una postura consciente, crítica y reflexiva, que incluya la pluralidad de voces, perspectivas y construcciones de sentido.

Empatía y el rol adulto en un mundo mediado por lo digital

El uso masivo de las tecnologías de la información y la comunicación es todavía algo novedoso e impactante para la mayoría de los adultos, quienes vieron transformadas y atravesadas sus cotidianidades por las diversas experiencias y aprendizajes digitales. Forzados por diversas circunstancias o por voluntad propia, la mayoría debió aprender aspectos básicos del funcionamiento de aplicaciones, redes sociales y sitios para acceder a nuevas posibilidades o a antiguas prácticas con nuevas modalidades. Uno de los grandes desafíos de la

actualidad radica en el desarrollo de un rol activo de los adultos en el acompañamiento y cuidado de los más jóvenes en Internet.

Las TIC, sin embargo, no son una novedad para aquellos que nacieron con ellas. Aunque las hayan utilizado poco, mucho o nada, su mera presencia naturaliza su práctica, volviéndose parte de su realidad. La naturalización de las tecnologías digitales como parte del entorno y de la vida cotidiana produce una diferencia generalizada entre adultos y niñas, niños y adolescentes denominada brecha generacional.

Uno de los principales efectos de esta brecha o distancia respecto del uso de las tecnologías digitales es la falta de empatía por parte de los adultos. Sea en el rol de padre, madre, docente, cuidador, familiar o amigo, el adulto suele pensar las temáticas, tensiones o problemáticas digitales a partir de sus propias visiones y definiciones, sesgadas por su experiencia de vida y su propio uso de las tecnologías digitales. La imposibilidad de ponerse en el lugar del otro (en este caso de las niñas, niños y adolescentes) se evidencia en las distintas problemáticas sociales que confluyen en los espacios digitales, como por ejemplo: *ciberbullying*, *grooming* o la viralización de imágenes. Frente a estas acciones cotidianas de la *web*, a las que los jóvenes están permanentemente expuestos, los adultos en general suelen tomar posturas desde sus propias concepciones o construcciones de sentido. Es decir, padres, madres y docentes carecen en general de capacidades para abstraerse y tener una mirada contextual que incluya los pareceres de los chicos y las chicas, y encaran estas problemáticas, cuando lo hacen, desde una mirada adultocéntrica. Un ejemplo de ello podría darse ante un caso de discriminación en Internet: se puede ver con frecuencia cómo los adultos minimizan o relativizan un conflicto que puede llegar a suceder en estos espacios, indicando que esas acciones siempre sucedieron en la sociedad, y que los jóvenes deben restarle importancia y resolverlo de manera sencilla o dejando de utilizar la aplicación o red social donde se observó el conflicto.

La principal consecuencia de esta falta de empatía es la carencia de sensibilidad a la hora de acompañar los trayectos digitales (y sociales) de los chicos y las chicas, alejando la posibilidad de que ellos los ubiquen como referentes de cuidado y contención. Cuando un adulto minimiza situaciones planteadas como conflictivas por los jóvenes, o pretende solucionarlas desde la restricción en el uso de dispositivos digitales, tiene

como principal efecto extender la distancia entre ambos y sobre todo, no solucionar o en algunos casos empeorar las situaciones expuestas.

Cabe destacar que las tensiones o problemáticas que suceden en el mundo digital son cuestiones sociales, relacionales o vinculares y que es desde esta arista donde los adultos en general pueden intervenir o participar. No hace falta ser un experto en lo técnico de Internet para tener un rol activo. Valiéndose de sus trayectorias personales y antiguos saberes es que padres, madres, familiares y docentes podrán inaugurar espacios de diálogo junto con los más jóvenes. Para eso es necesario escuchar e incorporar la voz de los chicos y las chicas, así como también sus percepciones, sentimientos y construcciones de sentido. En otras palabras, involucrar a los jóvenes en estos debates. Esta premisa es fundamental para poder acompañar los conflictos que veremos a continuación: la violencia digital, el *grooming*, la viralización de imágenes sin consentimiento y la construcción de reputación *web* o identidad digital.

Conflictos socio-digitales

Violencia digital

La burla, la discriminación, el hostigamiento o los discursos de odio son todas manifestaciones conductuales del ser humano que preceden a Internet. Sin embargo, los espacios digitales pueden devenir en potenciadores de estas situaciones o prácticas preexistentes. El *ciberbullying* o ciberhostigamiento es una de las violencias digitales más comunes en los relatos de las niñas, niños y adolescentes. El *bullying* digital se presenta como el acoso sistemático repetido en el tiempo, entre pares y mediante medios digitales. A su vez, muestra dos fenómenos a tomar en cuenta: el alcance y el efecto. Ambos suelen amplificarse, llegando a difundirse entre una cantidad mayor de personas por un lado, y por el otro provocando mayor intensidad en sus consecuencias para la eventual víctima. Este tipo de acoso a través de medios digitales también cuenta con otros agravantes a tener en cuenta. Por un lado, la exposición de la víctima todos los días y a toda hora al hostigamiento, sin posibilidad de descanso o interrupción. Por otro, la distancia física entre acosador y acosado, que puede volver aún más violentos o agresivos los mensajes o

conversaciones. La falta de registro del otro, de su mirada, voz y cuerpo puede generar una violencia aún más potente.

Conocer las características del hostigamiento digital o *ciberbullying* debe servir para comprender la dimensión del fenómeno y evitar minimizarlo. En ese sentido, padres, madres, docentes y tutores, en tanto adultos, deben abordar esta problemática. Es decir, no se puede mirar para el costado y eludir la responsabilidad. Ninguna excusa es válida, ni siquiera las que con frecuencia se escuchan desde estos públicos como por ejemplo: "de Internet no sabemos nada, no podemos conversar con nuestros hijos/alumnos sobre ello, porque ellos saben más".

La principal consecuencia para una niña, niño o adolescente víctima del ciberhostigamiento es la sensación de soledad. Es entonces clave que los adultos no potencien este sentimiento, sino que acompañen con empatía a quienes lo sufren.

Fomentar la convivencia digital

Una de las estrategias posibles para reflexionar y debatir con jóvenes acerca de esta problemática es mediante metodologías de trabajo en grupo. Es decir, para el trabajo de concientización sobre las problemáticas de *bullying-ciberbullying* se propone trabajar sin etiquetar a la víctima ni al victimario de un conflicto, e incluyendo a todo el grupo para la resolución del conflicto. En efecto, cualquier conflicto de *bullying* es el síntoma de tensiones grupales que deben abordarse como tales. La premisa debe ser el desarrollo de un espíritu colectivo en el que predominen el respeto y la empatía.

Entonces bien, lo primero debe ser cuidar y velar por los derechos individuales, pero luego también respetar los de los demás. En otras palabras, se deben formar ciudadanos conscientes y empáticos en Internet.

A su vez, es necesario identificar a un actor principal en esta problemática: *el público espectador*. Los usuarios que *a priori* no participan de un caso de hostigamiento, es decir no son los que producen el hecho, ni quienes lo reciben, pero sí son aquellos que con sus acciones –darle "me gusta" a una publicación, compartiéndola o haciendo comentarios– u omisiones –siendo pasivos y perpetuando el caso– no hacen más que amplificar o mantener el alcance y el efecto del acto. Plantear la reflexión desde este enfoque permitirá trabajar con todo el

grupo, ya que nadie queda exento de responsabilidad cuando se habla de *bullying* o *ciberbullying*. Así es que se podrá fomentar una conciencia crítica colectiva, en donde chicos y chicas se sientan involucrados/as y con el compromiso de intervenir.

Ahora bien, para poder dar una respuesta integral y pragmática a esta problemática que aqueja a espacios en donde transitan niños, niñas y adolescentes, como es la escuela, es necesario preguntarse ¿qué tipo de valores son los que queremos enseñar? Si buscamos educar, formar y no solo instruir, si reconocemos que el crecimiento de una persona autónoma y responsable en el plano moral es prioritario, si buscamos la construcción de un comportamiento ético o si buscamos en resumen acompañarlos en la larga conquista de la autonomía y la responsabilidad, resulta fundamental la presencia activa del adulto en espacios sociales como Internet o las redes sociales.

Prevención

Los chicos y chicas víctimas de *ciberbullying* suelen manifestar cambios en su conducta, principalmente angustia o tristeza. Es probable que sufran variaciones en su rendimiento escolar y que busquen mantenerse al día en forma constante de lo ocurrido en Internet para controlar las publicaciones que hacen sobre ellos. El encerrarse y buscar estar solos también puede ser un síntoma para tener en cuenta.

Es por eso que los adultos deben estar atentos a los cambios que se producen en el ánimo o conducta de los más chicos para poder ayudarlos y acompañarlos.

Cuando se interviene, es necesario promover espacios de reflexión con alumnos, docentes y familiares acerca de las prácticas sociales que modelan las diferentes formas de vinculación y la necesidad de cuidado. Es importante explicarles a los jóvenes las consecuencias de la discriminación en la *web* para que comprendan las responsabilidades de sus acciones. Muchas veces se supone erróneamente que es menos doloroso que el hostigamiento personal. Por eso es importante trabajar con todos los perfiles implicados: quienes agreden, quienes son agredidos, quienes son observadores y quienes son cómplices. En estos casos, se debe profundizar la responsabilidad sobre las propias acciones y sobre la necesidad de ser sujetos responsables también en Internet.

En todos los casos, como adultos debemos pasar a una situación activa y trabajar junto con los chicos y chicas en prevenir este tipo de conductas. Para eso se recomienda:

- Dialogar. Charlar de forma abierta con los niños y niñas y permitirles expresar lo que les ocurre. Esto es indispensable para detectar en forma temprana los casos de ciberacoso. Y remarcar que es importante no hacer o decir en Internet lo que no harían o dirían en persona.
- Promover el conocimiento. Alentar el diálogo sobre el tema con amigos o cercanos, ya que mantener la situación en secreto potencia tanto sus consecuencias como su aislamiento.
- Desalentar la difusión de actos discriminativos hechos por terceros o el reenvío de mensajes ofensivos.
- Participar en las redes sociales. Ser parte de la educación sobre buenas prácticas en Internet, estableciendo perfiles privados y eligiendo como amigos solo a personas que realmente conozcan.
- No responder con el mismo odio o violencia. Es necesario educar respecto a que la violencia genera más violencia, y si respondemos al odio con más odio, será un camino de ida hacia una situación muy agresiva.
- Utilizar las herramientas propias de Internet. La *web* ofrece formas de denuncia y bloqueo que deben conocerse y utilizarse. Es importante empoderarse de dichas herramientas para evitar maltrato y agresión. Cada plataforma que usemos tiene estas opciones, es indispensable identificarlas y conocer su uso.
- Educar en el respeto hacia el otro en todos los ámbitos. Los programas educativos y la crianza en los hogares deben incluir los valores de respeto, tolerancia y empatía hacia el otro. Es la única forma de evitar este tipo de expresiones.
- Fomentar una actitud activa. Internet no solo ofrece espacios de denuncia, sino que es en sí mismo un espacio de comunicación. Por ende, se debe propiciar una actitud proactiva a la hora de denunciar o llamar la atención ante episodios de agresión u odio. Quien observa este tipo de discurso debe poder expresarse en contra, utilizando los diversos canales de comunicación *online* que existen. Este tipo de postura también debe ser parte de la educación y crianza de las niñas y los niños.

Acción

Ante un caso de *ciberbullying*:

- Escuchar respetuosamente siempre a los jóvenes: el relato puede darse en primera persona o puede que un tercero hable acerca de una situación de hostigamiento tanto en el espacio escolar, el espacio extraescolar o el espacio digital. No actuar sin escuchar las necesidades de la niña o del niño. Una respuesta que no tenga en cuenta lo que los jóvenes necesitan puede exponerlos aún más y potenciar la humillación que sienten. Es por eso que si bien es indispensable que el adulto acompañe, debe consensuar reglas de acompañamiento.
- Acompañar. No minimizar ni exagerar la situación, aceptando lo ocurrido desde el acompañamiento.
- No demonizar la herramienta. Evitar echarle la culpa a Internet ya que los comportamientos *online* se condicen con los *offline* y la *web* es solo un medio para llevarlos a cabo.
- Bloquear usuarios indeseados. Cuando un contacto hostiga a un chico o a una chica se lo puede bloquear impidiendo así que vea sus perfiles, que lo contacte o que vea sus publicaciones.
- Realizar denuncias dentro de las plataformas utilizadas: las redes sociales tienen espacios de denuncia contra publicaciones o perfiles que deben ser utilizados por los usuarios para ejercer sus derechos. Es importante que los jóvenes sepan que esta denuncia es anónima.
- Guardar las evidencias. Internet ofrece formas muy efectivas, como las capturas de pantalla, que se utilizan a la hora de denunciar. Es importante dirigirse, en lo posible, a instituciones que se especialicen en delitos informáticos.
- Intervenir. Si la situación trasciende las redes y llega a la violencia interpersonal, ya sea agresiones físicas y/o verbales, es necesario que un adulto intervenga para atenuar los hechos. Si hubiera una pelea, por ejemplo, el adulto debe desarticularla disuadiendo a los intervinientes y calmándolos.

Grooming

El *grooming* es el contacto con fines sexuales de un adulto a una niña, niño o adolescente a través de espacios digitales. Es un tipo de abuso sexual y en nuestro país está tipificado como delito en el Código Penal.

Es conveniente reconocer que –lamentablemente– tanto la pedofilia como el abuso adulto son prácticas delictivas que preceden al uso masivo de las TIC, pero que sin dudas encuentran en la *web* plataformas que otorgan ciertas facilidades: anonimato, posibilidad de generar perfiles falsos, herramientas para acceder a datos personales de los niños y niñas, espacios con ausencia adulta, entre otros.

Es clave marcar los antecedentes históricos de esta problemática para identificar que no son las tecnologías digitales en sí las causantes del *grooming*, sino que esta es una práctica social que encuentra en las TIC medios para amplificar su alcance. Esta aclaración es relevante a la hora de pensar soluciones y medidas preventivas. Sin esta claridad se suele confundir el medio con la causa y así atacar o prohibir el uso de espacios digitales como forma de evitar un problema que los excede.

Empatía en *grooming*

Cuando existe un alerta o un caso de *grooming*, niñas, niños o adolescentes suelen sentir vergüenza de contárselo a sus padres o docentes. Según estadísticas de UNICEF en el estudio "Kids Online", solo un 9% de los jóvenes acudiría a un docente en casos de conflictos en la *web* y un 30% a sus padres. El resto prefiere compartirlo con pares. Estos números son alarmantes porque hablan de los pocos canales reales de comunicación tendidos entre los adultos, tanto en sus roles de educadores como de familiares, y los chicos y chicas.

En los talleres realizados por la ONG Faro Digital durante 2017 y 2018 se corroboraron estas estadísticas. Los estudiantes con los que se trabajó evidencian no recurrir a docentes ante problemas digitales debido a la falta de confianza o a la sensación de vergüenza. Muchos en cambio creen que consultarían con sus padres o familiares ante un caso de suma gravedad, atravesando la vergüenza generada. Es importante la observación de que en dichos casos, el contacto con los padres se ubica únicamente como última instancia, cuando ya no se encuentran soluciones entre sus pares sin intervención adulta.

Fases del *grooming*

El mecanismo del *grooming* consta de varias fases o etapas y suele comenzar con el establecimiento del contacto. Esto se puede dar mediante una red social, plataforma de *chat* o bien en un videojuego *online*. Una vez que se establece el contacto, se pasa a la fase de construcción de la confianza. Es decir, se genera un vínculo de amistad, muchas veces reforzado por las propias publicaciones de los chicos y las chicas en sus redes sociales. Es decir, se utilizan los gustos y preferencias por ellos compartidos para generar una sensación de cercanía y amistad. Esta fase puede durar días, semanas o meses. El hecho de que un chico o una chica esté en contacto por un tiempo extendido con un amigo *online* y este no haya hecho ningún pedido o extorsión, no es garantía de que no lo vaya a hacer después. Se registran casos donde el tiempo esperado por el abusador para extorsionar o abusar llega hasta un año o más.

Luego de la fase de amistad o generación de confianza, comienza la etapa del pedido. Puede ser una foto o video de índole sexual o erótica o una confesión o secreto. Cuando consigue ese material el abusador amenaza con hacer pública esa información si el menor no entrega nuevos videos o fotos o si no accede a un encuentro personal.

Como se dijo anteriormente, las TIC son herramientas que brindan nuevos escenarios para problemáticas previamente existentes. Es decir, el abuso o acoso sexual a chicos o chicas y la pedofilia no surgen con Internet y las redes sociales, ya que estas son problemáticas que anteceden la existencia de estos espacios. Lo que sí sucede es que se constituyen en instrumentos capaces de potenciar los distintos tipos de abuso.

Cabe destacar que en Argentina el *grooming* es un delito penado por la Ley N° 26904 e incluido en el Código Penal. La penalización incluye prisión de 6 meses a 4 años a quien por medio de comunicaciones electrónicas, telecomunicaciones, o cualquier tecnología de transmisión de datos, contacte a una persona menor de edad, con el propósito de cometer cualquier delito contra la integridad sexual de la misma.

Prevención

A continuación detallamos algunos puntos que los adultos deben trabajar con niñas, niños y adolescentes:

- Como ya dijimos anteriormente es fundamental tener una actitud activa y presente. Es necesario que los padres, madres y

docentes incorporen a la crianza y al diálogo cotidiano la vida *online* de sus hijos o estudiantes en su propia vida *online*. El conocimiento sobre las páginas *web*, redes sociales, aplicaciones que usan frecuentemente y las personas con quienes interactúan los chicos y las chicas es indispensable.

- Es fundamental a su vez que esta presencia y compañía se construya desde antes que los chicos y las chicas utilicen por primera vez dispositivos digitales. Es clave que haya un recorrido previo, protagonizado por la charla y el debate antes de decidir darle a las niñas y los niños acceso a las tabletas, celulares o computadoras. Se debe incorporar el mismo mecanismo que ocurre con cualquier otro primer uso: explicación y diálogo previo.
- Acompañar a los jóvenes. Si bien los adultos sienten muchas veces que saben menos que sus hijos o hijas respecto del uso de las TIC, esto no debe evitar que los acompañen. Para los jóvenes es clave sentir que pueden confiar en sus adultos de confianza y compartir sus experiencias. En estos casos vale tener en cuenta que el acompañamiento adulto eficaz para una niña o un niño tiene que ver con la contención, interés, presencia y empatía y no tanto con saberes digitales ni informáticos.
- No es necesario tener todas las respuestas. Puede suceder que un niño o una niña recurra a un adulto ante casos de *grooming* y este no sepa cómo actuar. Este desconocimiento no debe ser causa de no intervención. Se deben buscar actores capacitados que ayuden a los padres o docentes a llevar adelante el tema, con un asesoramiento que complemente esa falta de conocimiento primaria.
- Distinguir entre niños-niñas y adolescentes. Seguramente la presencia requerida y necesitada por los más chicos sea distinta que la de los adolescentes. No es lo mismo el contacto con extraños, tanto en espacios digitales como personales, para un niño o una niña que para un joven. Por eso es necesario con los chicos y las chicas de nivel primario tener un contacto y comunicación diarios respecto de sus usos digitales, y en muchos casos, un grado de control más específico. Los adolescentes seguramente necesiten espacios sin intervención adulta e incluso los busquen y generen. Allí las estrategias deben

ser otras, basadas más en la confianza construida previamente y en el diálogo que en el control.

- Comparar los inicios con otras actividades. En estos casos, los adultos sienten mucha incertidumbre ante la pregunta de cuándo es la mejor edad para el inicio de la participación en los espacios digitales. Es importante entonces comparar con cómo se tomaron otras decisiones similares: ¿a qué edad los jóvenes pueden volver solos del colegio?, ¿a qué edad están listos para cortar con cuchillo?, ¿para cruzar la calle solos? Para este tipo de preguntas no hay una única respuesta, sino que cada padre o madre lo resolverá según la madurez del chico y la relación que tengan con él o ella. En Internet ocurre lo mismo: los padres desde su presencia y conocimiento deben pensar para qué está listo su hijo o su hija. En cualquier caso, creemos que la participación debe ser desde la educación y la compañía.
- Trabajar la noción de anonimato y falsa identidad en la *web*, explicándoles lo sencillo que es abrir un perfil con datos falsos. La identidad en Internet no es fácil de corroborar como lo es en el contacto cara a cara. Los chicos y las chicas que nacieron con un universo donde los amigos y las amigas pueden ser tanto los del colegio o los del barrio, como los del *chat*, Facebook u otra red social, en muchos casos no distinguen las diferencias entre estos.
- Comprender que la información que se vuelca en Internet puede caer en manos de personas con malas intenciones. Por esa razón, es indispensable cuidar quién ve las publicaciones utilizando las configuraciones de privacidad de las redes sociales. Cuando abrimos una cuenta (en cualquier red), las publicaciones están por defecto públicas. Por ese motivo es importante tomarse el trabajo de configurar la privacidad y así elegir que sean solamente nuestros contactos los que estén habilitados a ver el material publicado. Cuando se indaga en las herramientas de privacidad nos encontramos con opciones más avanzadas aún: armar subgrupos entre los contactos y elegir qué cosas ve cada grupo, restringir las etiquetas antes de que se publiquen en nuestros muros, bloquear un perfil, entre otros.

- No dar información o imágenes comprometedoras en Internet. Esta recomendación no debe limitarse a los desconocidos, ya que las fotos rápidamente pueden cambiar de contexto y quedar expuestas en la *web*. Es importante reforzar la idea de que el material que circula en Internet es difícil de borrar. Como ya se dijo, si alguna imagen íntima comienza a circular, va a verse asociada en el presente y en el futuro con las búsquedas *online* de la persona que protagonice el video o la foto, no importa si este material se envió a un conocido; puede trascender y quedar en la *web* por mucho tiempo y luego ser utilizado públicamente para dañar la imagen de quien lo envió.
- No utilizar la cámara *web* cuando chatean con desconocidos. Del otro lado pueden estar grabando lo que ellos o ellas muestren, tenga o no contenido sexual. La imagen forma parte de la identidad digital y requiere cuidado y protección. Mostrarse a través de una cámara *web* es una forma de entregar material a un desconocido que puede hacerlo circular por la *web* o utilizarlo para futuras extorsiones.
- No utilizar el nombre completo en el usuario cuando se juega *online*. Es preferible colocar sobrenombres y evitar el apellido para impedir que desconocidos accedan a información personal.
- Saber cómo configurar la privacidad y la seguridad de las cuentas, para así poder realizar estas acciones junto a los chicos y chicas y poder elegir con quién comparten la información que publican.
- Evitar que les roben la información comprometedora. Para eso es necesario configurar y mantener la privacidad y seguridad de los dispositivos.

Acción

Ahora bien, si detectamos que un niño o una niña está siendo víctima de *grooming* es necesario que como adultos actuemos de manera rápida y efectiva. Es por eso necesario:

- Guardar las pruebas del acoso. Es necesario no borrar conversaciones y fotografiar o capturar la pantalla y almacenar esta información en algún dispositivo. Sumado a esto, se deben

guardar los *links* (URL –*Uniform Resource Locator*–) de los sitios en donde el acoso se manifiesta. Las fotografías o los videos enviados por el acosador podrán proveer datos útiles para una futura investigación (marca, modelo y número de serie de la cámara, fecha y hora en la que se tomó la foto o el video, si fue retocada, el programa usado para hacerlo y datos sobre la computadora donde se la cargó, etc.).

- Limitar la capacidad de acción del acosador al detectar el caso de *grooming*. Como es posible que el acosador haya tenido acceso al equipo del chico o la chica o que tenga sus claves personales, recomendamos revisar el dispositivo (computadora, tableta o teléfono celular) y cambiar las claves de acceso, revisar y reducir las listas de contactos de las redes sociales como así también configurar la privacidad en cada una de estas.
- Analizar el tipo de delito que se llegó a cometer. No es lo mismo si hubo un encuentro personal o si no se traspasó la *web*. Estos datos serán importantes a la hora de pensar en hacer una denuncia policial.
- Hacer la denuncia penal. Aunque la decisión de realizarla parte del chico o la chica que sufrió el abuso y de su familia, es necesaria la intervención adulta que deje en claro que denunciar ayudará a generar justicia para la víctima, así como también para el resto de los potenciales afectados. La importancia de la denuncia hay que enmarcarla no solo en el delito cometido, sino en la certeza de que los abusadores no suelen atacar a una sola víctima, sino que actúan sobre varios chicos o chicas. Denunciando en comisarías o fiscalías se logra que se investigue y penalice, evitando que el abusador continúe perjudicando a otros niños o niñas.

Difusión de imágenes sin consentimiento

La difusión de una foto o un video sin permiso suele comenzar por el envío en forma privada, sea por *chat* o *e-mail*, de un contenido íntimo, por lo general sexual o sensual. Este envío, enmarcado en la privacidad, suele tener como contexto una relación de confianza que supone la no difusión de esas piezas. Sin embargo, por diversos

motivos que veremos luego, alguna de las partes difunde, sin permiso del o la protagonista, el material en espacios públicos de la *web*.

Una vez que una foto o un video íntimo comienza a circular entre distintas plataformas y dispositivos, su distribución es difícil y a veces imposible de detener. Aunque la persona que difundió en primera instancia el material lo borre, nada asegura que terceras personas no lo hayan descargado o guardado la captura de pantalla para seguir compartiéndolo. Esta difusión es un fenómeno que sucede con frecuencia en la actualidad, no solo en jóvenes sino también en adultos.

El principal riesgo en los casos de difusión es el fenómeno denominado viralización, que sucede cuando un material es compartido en forma masiva por diversos usuarios en diversas plataformas con altas cantidades de reproducciones o compartidas.

Para comprender este fenómeno debemos abordar la práctica de "sextear", es decir, enviar una imagen sexual personal mediante chats o mensajes de texto. Esta práctica está muy instalada en jóvenes y también en adultos y en principio, si ambas partes están de acuerdo, no debería ser causa de problemas.

En efecto, el problema surge cuando esa foto o video que se envió mediante la práctica del "sexting" se difunde sin permiso. Es decir, la responsabilidad nace en la persona que se registra y envía el contenido a otro, pero sobre todo en quien recibe ese material y decide amplificar su alcance.

Es importante reconocer que quien se filma o toma una foto decide exponerse a una pérdida de control de sus datos personales debido a las particularidades de Internet, pero no por eso se puede señalar como una práctica que en sí misma genere el conflicto. Las nuevas generaciones nacieron con estas tecnologías, en una época de "extimidad", haciendo que sus construcciones de sentido y definiciones de lo privado y de lo público difieran de las previas concepciones. Es preciso comprender estas percepciones para poder desarrollar empatía con los jóvenes y así poder acompañarlos y cuidarlos.

La problemática surge cuando una foto o un video es compartido con uno o muchos, sin que el titular del dato lo quiera o haya expresado su consentimiento. Una vez que sucede esto, el efecto viral es muy difícil de detener. Es por eso que se habla de desarrollar empatía. Ya

que la constante viralización de imágenes genera un daño en la reputación, honor e imagen de las personas.

En los talleres con jóvenes realizados por Faro Digital se han detectado diversas estrategias que estos utilizan en algunos casos y que resultan útiles a la hora de darles herramientas para proteger su privacidad y sus derechos ante esta problemática. En primera instancia debemos comprender como adultos que la pubertad y la adolescencia son etapas de exploración sexual y que las actuales generaciones transitan su vida social atravesadas tanto por cámaras de celulares como de una gran primacía de la imagen. En ese sentido, es lógico y esperable pensar que exploren sus sexualidades a través de fotos y videos tomados por ellos mismos. Teniendo en cuenta que la práctica de sacar fotos o filmar videos íntimos es habitual en los más jóvenes, la disminución de riesgos surge como un camino posible a tomar. En efecto, aconsejar que no se saquen fotos sería obviar una realidad muy difícil de modificar, e incluso culpabilizar a las víctimas que tienen derecho a enviar fotos de su cuerpo.

Dentro de las estrategias para reducir riesgos, los jóvenes identifican la posibilidad de anonimizar las imágenes al compartirlas con un mecanismo que posibilita realizar la práctica cuidando sus datos personales. Esto es, quitando los elementos distintivos de las mismas, como ser: la cara, marca de nacimiento, tatuaje, collares, pulseras, etc. A esto se pueden sumar algunas herramientas técnicas que permiten aumentar la seguridad de los dispositivos, como el uso de carpetas encriptadas con códigos de acceso, mensajerías con cifrado de punto a punto o también contar con políticas de contraseñas efectivas.

Prevención

Producir imágenes, editarlas y compartirlas son algunas de las posibilidades que ofrecen las tecnologías digitales. En este sentido, la solución a los problemas asociados con el *sexting* no proviene de prohibirles a las niñas, niños y adolescentes que se saquen fotos y se filmen, sino de dialogar sobre las posibles consecuencias de estas prácticas, ente otras cuestiones.

A continuación, algunas recomendaciones:

- Inmersos en la dinámica del presente absoluto, las ninas, niños y adolescentes no desarrollan por sí mismos estrategias

de análisis crítico o conceptual, ya que para eso necesitan de los adultos. Por eso se vuelve imprescindible abrir el debate sobre la diferencia entre lo público y lo privado. Es recomendable indagar sobre las definiciones de privacidad de los chicos y chicas, y remarcar la importancia de cuidar aquello que se considera privado o íntimo, entendiendo a lo privado como propio. En ese sentido, así como se cuida un objeto material, se debe cuidar la información privada. Cabe aclarar en este punto que es esperable y propio del desarrollo emocional y cognitivo de los niños y las niñas que no cuenten con un tipo de análisis crítico o conceptual; esta es una tarea que los adultos no pueden relegar. Es necesario pensar antes de enviar datos personales, como fotos o videos con contenido sexual, ya que, una vez enviados, se pierde el control sobre su recorrido. Al compartir este tipo de materiales, debemos acordarnos de que pueden caer en manos de personas con malas intenciones que los distribuyan o incluso los editen y los hagan circular.

- Recordarles que deben evitar compartir, reenviar o difundir fotos o videos con contenido sexual de personas que no brindaron su consentimiento. Como adultos tenemos la responsabilidad de inculcar prácticas de respeto al otro también en la *web* y, por lo tanto, educar a los chicos y las chicas sobre lo importante que es preservar la imagen de los demás y evitar publicar o compartir materiales que la puedan comprometer.
- La utilización de contraseñas seguras ayuda a cuidar la información privada que esté alojada en dispositivos móviles. Teléfonos celulares, tabletas, *notebooks* y *netbooks* deben contar con sistemas de bloqueo, para evitar que personas indeseadas accedan a los materiales guardados. Las contraseñas seguras están formadas por una combinación de números, símbolos y letras mayúsculas y minúsculas. Para mayor efectividad, deben ser cambiadas periódicamente, y evitar compartirlas.
- Si se decide no usar la cámara *web* mientras se chatea, se recomienda taparla. Activar en forma remota una cámara *web* y capturar imágenes es una tarea sencilla. Por eso, se recomienda taparla para evitar que se tomen imágenes en contra de la voluntad de la persona.

- Realizar una copia de seguridad de las fotos y borrarlas de los teléfonos celulares, tabletas o netbooks. Estos dispositivos pueden ser olvidados, robados o llevados a reparación y, por lo tanto, caer en manos de desconocidos, por lo que es recomendable no guardar en ellos información privada.

Acción

Cómo actuar frente a la circulación de las imágenes en Internet:

- Reportar siempre las imágenes sexuales en la *web* de niñas, niños y adolescentes. Es una buena forma de cortar con su circulación. Tanto en redes sociales como en sitios de videos o blogs, contamos con opciones de denuncia y bloqueo de imágenes indebidas. Usarlas es una forma de ejercer nuestra ciudadanía digital. Tanto los adultos como los jóvenes debemos difundir y utilizar estas herramientas.
- En el caso de material sexual sobre niñas, niños y adolescentes, se puede realizar una denuncia en las comisarías o fiscalías cercanas, como así también asesorarse legalmente para denunciar la publicación.

Reputación *web*

Internet en general y los buscadores en particular constituyen en la actualidad las cartas de presentación de las personas ante el mundo. La *web* es el espacio público en donde todos quienes tienen acceso pueden conocer información acerca de alguien. Por ende, toda la información que se sube o que suben otros a Internet forman la identidad digital de un usuario. Ahora bien, ¿qué información se muestra allí? ¿Cuál en las redes sociales? ¿Cómo construyen los usuarios sus perfiles? ¿Cómo eligen definirse? ¿Lo hacen de manera consciente? ¿Existe algún nivel de comprensión de la mirada del otro? ¿Qué se hace con ello? ¿Se utilizan estrategias para crear una identidad digital de manera activa?

Rol del adulto

Para que los niñas, niños y adolescentes comprendan la relevancia de estar construyendo su identidad en un espacio público –como son los

entornos digitales– es importante que los adultos dialoguen con ellos sobre una serie de conceptos clave para promover la concientización y lograr un uso responsable. Es importante, por eso, generar instancias de diálogo sobre la construcción de la identidad digital como algo que los acompañará toda su vida y que puede tener consecuencias positivas o negativas en el presente y en el futuro. También es necesario hablar sobre el contenido que deben y no deben compartir públicamente y ayudarlos a respetar la privacidad de los demás.

- La información que está en Internet es la carta de presentación ante personas desconocidas. Ellas buscarán qué datos o referencias pueden encontrar en la *web*.
- Introducir y debatir sobre el derecho al olvido. Reflexionar junto con los chicos y las chicas acerca de que la información que se publica es difícil de borrar, por lo que es conveniente pensar antes de publicar o compartir cierta información.
- Debatir sobre la diferencia entre los espacios públicos y privados. Explicar entonces la relevancia de utilizar los mecanismos técnicos que las redes sociales ofrecen para publicar información, pero restringiendo el público que puede acceder a ellas. Para eso es fundamental recomendar a los jóvenes que configuren sus cuentas y preserven su privacidad e intimidad.
- Configurar la privacidad en las redes sociales que se utilicen para establecer que solo los contactos que se desee vean todas las publicaciones, tanto del pasado como del presente. De esta forma, se puede evitar que desconocidos vean sus posteos, fotos o videos.
- Si el usuario agrega a desconocidos en las redes sociales, es conveniente tener mayor cuidado en la información que se publica ya que esa persona puede tener otras intenciones con los datos y la información, e intentar reproducirlos.
- Pensar antes de publicar. Tener siempre en cuenta que en Internet no existe el olvido y, por consiguiente, después de publicar algo se puede perder el control sobre lo subido.
- Controlar qué información personal circula en Internet. Existen herramientas de los buscadores que funcionan como alertas que pueden avisar que un usuario es nombrado/a y así informar cuando esto sucede. Es un buen ejercicio también

poner nombre y apellido en los buscadores cada cierto tiempo para saber qué se dice de uno en la *web*.

- Colocar contraseña en los celulares u otros dispositivos para evitar que otra persona pueda acceder a la información, a las fotos, a los videos o a los mensajes que se guardan en ellos. Esa persona puede querer publicar, por diversos motivos, esa información privada en la *web* y afectar la reputación o identidad del usuario.
- Utilizar contraseñas seguras, fáciles de recordar pero difíciles de adivinar. Es importante no compartirlas y modificarlas cada cierto tiempo. La computadora, el celular, las cuentas en redes sociales, blogs, foros o *e-mails* contienen información que cada usuario debe cuidar. Si caen en manos de otras personas, puede publicarse algo que uno no elegiría hacer público.
- Tener en cuenta que los "amigos *online*", por más cariño que se les tenga, son desconocidos. Eso no significa que se tenga que dejar de hablarles, pero sí cuidar la información personal que se les da para evitar que la publiquen o difundan.
- Evitar colocar nombre y apellido en las producciones o publicaciones que el usuario no quiere que se asocien con su identidad. Es recomendable utilizar seudónimos en estos casos.

El camino es entonces no subestimar a los chicos y las chicas e incluirlos en los debates. Escucharlos y darles espacio para que puedan incorporar herramientas que fomenten la reflexión sobre la información que comparten de su vida social en Internet. Es importante ayudarlos a deconstruir sus hábitos y a formarse de manera consciente para que logren debatir y decidir sobre su identidad digital.

Conclusiones

Cuando los jóvenes se saben escuchados y valorados es que se logra tener instancias de participación activa en los procesos de educación digital como talleres, clases o debates.

En los diversos talleres y entrevistas en profundidad llevadas adelante por Faro Digital, observamos la necesidad de parte de las niñas,

niños y adolescentes de tener canales empáticos de comunicación con los adultos respecto de sus experiencias digitales. Esos canales deben abrirse antes del inicio de sus actividades *online*, mantenerse y actualizarse en el tiempo. Asimismo, es necesario que esas conversaciones no giren únicamente alrededor de aspectos negativos o problemáticos presentes en la *web*, sino que también incluyan y profundicen en acciones que les gusten, diviertan, enseñen o enriquezcan.

Esto permite explorar los distintos usos de lo digital, las percepciones de sus protagonistas, los códigos que se crean, los debates grupales que surgen, las situaciones incómodas o negativas que viven y también lo que les gustaría aprender en esos espacios.

Una vez que se logra desarrollar este tipo de experiencias es que se pueden extraer las conclusiones pertinentes para poder construir herramientas útiles para la ciudadanía en general, y para los padres y docentes en particular. De esta manera existirá un mayor entendimiento de la relación entre los jóvenes y las tecnologías. Algo que permitirá desde el punto de vista adulto amigarse con algo que le es *a priori* ajeno o difícil de entender, pero que en la actualidad es condición obligatoria para poder acompañar, educar y fomentar el desarrollo de niños y niñas.

No existe un botón que solucione mágicamente las tensiones que se generan en Internet. Lo positivo es que desde los antiguos saberes y la experiencia de vida de familiares, maestros y docentes se pueden hallar diferentes caminos posibles que acerquen al objetivo de conocer más a los jóvenes y sus realidades para poder ayudarlos.

Existen varios recursos para utilizar como charlas, debates, dinámicas lúdicas, exposición de videos, series o películas, y hasta es posible valerse de las TIC como medios –y no como un fin en sí mismas– para permitir la construcción de una convivencia social crítica en Internet y en las redes. Estas estrategias deben poner a los jóvenes en el centro de la escena, y velar por involucrarlos en las discusiones.

En suma, para poder concebir a Internet como un espacio de comunicación y diálogo es necesario que adultos (maestros, docentes, padres, madres y cuidadores) se hagan cargo de la situación actual y no miren para el costado. Asumir la responsabilidad del rol que se tiene y trabajar fuertemente todos los días.

Bibliografía

CÁCERES, Jesús, "Cibercultura, ciberciudad, cibersociedad: hacia la construcción de mundos posibles en nuevas metáforas conceptuales", Estudios sobre las Culturas Contemporáneas, Vol. IV, N° 7, junio de 1998.

GIONES, Aina y SERRAT, Marta, "La gestión de la identidad digital: una nueva habilidad informacional y digital", BID, N° 24, Universidad de Barcelona, Barcelona, 2010.

MENJÍVAR OCHOA, Mauricio, "El sexting y l@s nativ@s neo tecnológic@s: apuntes para una contextualización al inicio del siglo XXI", en Revista electrónica *Actualidades investigativas en educación*, Vol. 10, N° 2, mayo-agosto de 2010.

MORROW, Allison y DOWNEY, Christina A., "Perceptions of adolescent bullying: Attributions of blame and responsibility in cases of cyber-bullying", Scand J Psychol, Epub 2013.

PAOLINI, Paola y REVALLI, María Jose, "Kids Online, Chic@s Conectados, investigación sobre percepciones y hábitos en niños, niñas y adolescentes en Internet y redes sociales", UNICEF Argentina, junio de 2016.

PIERDANT PÉREZ, Mauricio, "*Ciberbullying*, *Grooming* and *Sexting*, los niños y adolescentes ante el Internet. ¿Dónde estamos los padres de familia y los pediatras?", *Pediatr Mex*, Vol. 15, N° 3, 2013.

RICE, Eric; RHOADES, Harmony; WINETROBE, Hailey; SANCHEZ, Monica [*et. al*], "Sexually explicit cell phone messaging associated with sexual risk among adolescents", *Pediatrics*, Vol. 130, N° 4, 2012.

SERRANO-PUCHE, Javier, "Vidas conectadas: tecnología digital, interacción social e identidad", *Historia y Comunicación Social*, Vol. 18, Número especial noviembre, 2013.