ERREIUS

SUPLEMENTO
ESPECIAL

CIBERCRIMEN Y DELITOS INFORMÁTICOS

Los nuevos tipos penales en la era de internet

AÑO 2018

Ciberdelitos | Fraude informático | Tenencia de pornografía infantil | *Grooming* | *Phishing* | *Hacking* | Protección de datos personales | Daño informático | *Sexting* | *Revenge porn* | *Sextortion* | *Stalking* | Evidencia digital | Seguridad informática | Dirección IP | *Deep web* | Identificación por radiofrecuencia | Informática forense | Políticas preventivas |

Anónimo
Cibercrimen y delitos informáticos : los nuevos tipos penales en la era de internet / compilado por Ricardo Antonio Parada ; José Daniel Errecaborde. - 1a ed . - Ciudad Autónoma de Buenos Aires : Erreius, 2018.
192 p. ; 26 x 19 cm.

ISBN 978-987-4405-56-2

1. Delitos Informáticos. I. Parada, Ricardo Antonio, comp. II. Errecaborde, José Daniel, comp. III. Título.
CDD 343.0999

ERREIUS

CENTRO DE ATENCIÓN PERSONAL:
PARANÁ 725 - (1017)
BUENOS AIRES - ARGENTINA
TEL.: 4370-2018
E-MAIL: clientes@erreius.com

www.erreius.com

ISBN 978-987-4405-56-2

Esta edición se terminó de imprimir en los talleres gráficos de BluePress SA, Buenos Aires, República Argentina en agosto de 2018

CIBERCRIMEN
Y DELITOS INFORMÁTICOS

SUPLEMENTO ESPECIAL

La creación de internet implicó la aparición de nuevos paradigmas en materia de procesos de comunicación masiva. Como consecuencia de tal hito, el derecho tuvo que readecuar sus instituciones a los fines de describir, predecir y regular las conductas sociales materializadas en los mencionados procesos, a través de herramientas que permitan reglamentar aquellas conductas que puedan resultar penalmente reprochables.

Bajo la comprensión de estos nuevos paradigmas, el presente suplemento aborda, por un lado, el estudio de los nuevos tipos penales, llamados "informáticos"; a la vez que analiza el cibercrimen y las herramientas para la efectiva investigación en entornos digitales.

Por otro lado, se examinan las características y problemáticas que representan las normas que regulan los delitos cometidos en nuestro país a través de medios digitales. En ese sentido, la ley 26388, sancionada en el año 2008, conocida como la ley de delitos informáticos, introduce nuevos tipos penales al Código Penal de la Nación vinculados al uso de la tecnología. Posteriormente se sancionó la ley 26904 -ley de *grooming*- para hacer frente al delito que afecta a gran cantidad de menores de edad; y la ley 27436, que penaliza la tenencia de pornografía infantil, modificando de ese modo al artículo 128 del Código Penal. La naturaleza peculiar de estas normas importa la exigencia a los operadores jurídicos de comprender las novedades y conflictos suscitados en la nueva era.

Asimismo son objeto de estudio las herramientas procesales destinadas a la investigación en entornos digitales y los problemas derivados de la producción y valoración de la evidencia digital.

Por ello, Erreius pone a disposición un suplemento especial con el análisis de reconocidos autores de la materia, con el objeto de brindar conocimientos necesarios tanto tecnológicos como jurídicos para la investigación de delitos en entornos digitales y así seguir aportando a nuestros lectores las herramientas que les permitirán entender el cambio en medios digitales.

Sumario

La estrategia gubernamental frente al cibercrimen: la importancia de las políticas preventivas más allá de la solución penal

Gustavo Sain(*)

I - BREVE HISTORIA DE LOS DELITOS INFORMÁTICOS

La vinculación entre tecnología y delito no comenzó con el desarrollo de las computadoras. Con el surgimiento del telégrafo durante el siglo XIX se interceptaban comunicaciones para la transmisión de información falsa con fines económicos. Ya con la irrupción del teléfono, durante la década del 60, diferentes programadores informáticos o especialistas en sistemas intentaban boicotear el financiamiento gubernamental a la guerra de Vietnam mediante el uso gratuito del servicio. Los *phreakers* (neologismo proveniente de las palabras en inglés *"freak"*, de rareza; *"phone"*, de teléfono; y *"free"*, gratis) utilizaban unas *blue boxes* o cajas azules que reproducían tonos de llamadas similares a los utilizados por la Bell Corporation, y la ATT establecía comunicaciones gratuitas de larga distancia. En cuanto a la utilización de computadoras, la principal preocupación estaba dada por el manejo de la información a partir del almacenamiento y procesamiento de datos personales producto de obras de ficción como 1984 de Orwell.(1)

(*) Licenciado en Ciencias de la Comunicación Social (UBA). Magister en Sociología y Ciencias Políticas (FLACSO-UNESCO). Asesor en Cibercrimen de la Dirección Nacional de Política Criminal del Ministerio de Justicia y Derechos Humanos de la Nación. Profesor titular en la Universidad Nacional de Quilmes (UNQ) y en el Instituto Universitario de la Policía Federal Argentina (IUPFA)

(1) Sain, Gustavo: "Cibercrimen: el delito en la sociedad de la información". En Eissa, Sergio (Coord.): "Políticas públicas y seguridad ciudadana" - Ed. Eudeba - Bs. As. - 2015

Las primeras conductas indebidas o ilícitas relacionadas con computadoras comenzaron a verse reflejados durante la década del 70, a partir de algunos casos resonantes retratados por los periódicos de época. Los primeros delitos informáticos eran de tipo económico, entre los que se destacaban el espionaje informático, la "piratería" de software, el sabotaje a bases de datos digitalizados y la extorsión. En relación con el espionaje, estos se llevaban a cabo mediante la extracción de discos rígidos de las computadoras, el robo de *diskettes* o copia directa de la información de los dispositivos, tanto así como la absorción de emisiones electromagnéticas que irradia toda computadora para la captación de datos. El espionaje era comercial o industrial, como suele denominarse, siendo sus principales objetivos los programas de computación, los datos de investigación en el área de defensa, la información contable de las empresas y la cartera de direcciones de clientes corporativas. En relación a la piratería de software, la modalidad característica era la copia no autorizada de programas de computadora para su comercialización en el marco del espionaje industrial. Los casos de sabotaje y extorsión informática eran los delitos que más preocupaban organizaciones ante la alta concentración de datos almacenados en formato digital.

En cuanto a los fraudes de tipo financiero, a fines de esa década y principios del 80, hubo casos de alteración de archivos de las bases de datos de las empresas y los balances de los bancos para la manipulación de facturas de pagos de salarios. Casos típicos se realizaban mediante la instalación de dispositivos lectores, en las puertas de entradas de los cajeros automáticos, y teclados falsos, en los mismos, para la copia de los datos de las tarjetas de débito a través de la vulneración de las bandas magnéticas. Esto motivó, por parte de las empresas emisoras, la adopción de chips, en los plásticos, como medida de seguridad[2]. *"Fue justamente durante esta época donde comienza la protección normativa de los países europeos a los bienes inmateriales como el dinero electrónico, proceso iniciado por Estados Unidos en 1978. La cobertura legal de las bases de datos de las instituciones bancarias y empresas resultaba indispensable para la realización de negocios, fundamentalmente contra el robo de información comercial".*[3]

Con la apertura global de internet, a mediados de los años noventa, por parte de la administración norteamericana, y el posterior desembarco de empresas y bancos a la red para el desarrollo del comercio electrónico, la industria editorial, discográfica y cinematográfica comenzó una afrenta contra la multiplicidad de casos de violaciones a los derechos de autor, a partir de la descarga e intercambio en línea de obras digitalizadas, música y películas protegidas bajo leyes de copyright. Asimismo, bajo la posibilidad de construcción de identidades ficticias que brindan los entornos virtuales en internet, un rebrote de pedofilia inundó la red mediante la distribución de imágenes de pornografía infantil. Asimismo, el tema de la protección a la intimidad y la privacidad de las personas comenzaron a ser una preocupación a partir del uso de nuevas tecnologías digitales en la red.

(2) Sieber, Ulrich: "El problema: tipos comunes de delitos informáticos". En Aspectos legales de los delitos informáticos en la sociedad de la información. Bruselas, Informe de la Comisión Europea - 1998

(3) Sain, Gustavo: "Evolución histórica de los delitos informáticos" - Revista Pensamiento Penal - 11/4/2015

II - CRIMINOLOGÍA DEL CIBERCRIMEN

Desde un punto de vista criminológico, existen dos enfoques, en cuanto a la naturaleza de este nuevo tipo de fenómeno criminal; el primero de ellos es que los delitos informáticos no son más que delitos convencionales que toman nueva vida a partir del uso de dispositivos informáticos y de servicios y aplicaciones en internet. La segunda perspectiva afirma que las tecnologías de la información y comunicación brindan nuevas herramientas para la comisión de delitos inexistentes, como la distribución de virus o programas maliciosos a través de la red, ataques a sitios web y la piratería del *software.* Lo cierto es que ambos enfoques son ciertos. Existen delitos tradicionales que adquieren nuevas formas a partir de la intermediación de dispositivos automatizados como también nuevas formas delictivas que no serían posibles de cometerse si no existiese un programa de *software* o archivos digitales presente, como, por ejemplo, en la elaboración de programas maliciosos con el fin de dañar un servidor web para afectar el funcionamiento de la página, o aquellos para extraer información de un dispositivo -por ejemplo, los *spyware* o programas espías-, o alterar o dañar el funcionamiento de un dispositivo a través de virus, gusanos y troyanos.(4)

¿Pero qué son los delitos informáticos? Si bien no existe una definición específica, desde la década del 70 esbozaron distintas acepciones en cuanto al alcance del término. Según el Manual de Recursos de Justicia Criminal del Departamento de Justicia de los Estados Unidos de 1979 se entienden por estas conductas a *"cualquier acto ilegal donde el conocimiento de la tecnología computacional es esencial para el éxito de su prosecución"*(5). Según una definición brindada por la Organización de Cooperación y Desarrollo Económico en 1983, el delito informático es "*cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesamiento automático de datos y/o transmisiones de datos"*(6). Para el Consejo de Europa, según una definición de 1995, es *"cualquier delito penal donde las autoridades de investigación deben obtener acceso a información que ha sido procesada o transmitida por sistemas computacionales o sistemas de procesamiento electrónico de datos"*(7).Para el criminólogo Majid Yar, la ausencia de una definición específica sobre el fenómeno del cibercrimen se debe fundamentalmente a que *"la delincuencia informática se refiere no tanto a un único distintivo tipo de actividad delictiva, sino más bien a una amplia gama de actividades ilegales e ilícitas que comparten en común el único medio electrónico (ciberespacio) en el que tiene lugar"*.(8)

Más allá de las definiciones existentes sobre este tipo de conductas, lo cierto es que *el cibercrimen no representa un tipo de criminalidad específica*, no es parte del crimen completo ni organizado, ni tampoco pueden ser considerados delitos de cuello blanco,

(4) Sain, Gustavo: "Delito y nuevas tecnologías: Fraude, narcotráfico y lavado de dinero por internet" - Editores del Puerto - Bs. As. - 2012

(5) Schjolberg, Stein: "*The history of global harmonization on cybercrime legislation. Road to Geneva*" - Documento web - pág. 8

(6) Estrada Garavilla, Miguel: "Delitos informáticos" - Universidad Abierta - México D. F. - año sin consignar - pág. 2

(7) Schjolberg, Stein: "*The history of global harmonization on cybercrime legislation. Road to Geneva*" - Documento web - pág. 8

(8) Yar, Majid: "Cybercrime and society" - Sage Publications - London - 2006 - pág. 5

de acuerdo con la definición brindada por Edwind Sutherlard en 1929[9]. En líneas generales, cuando se habla de delitos informáticos nos referimos a aquellas *conductas indebidas e ilegales donde interviene un dispositivo informático como medio para cometer un delito o como fin u objeto del mismo.* En este sentido, *los delitos informáticos son entendidos respecto al lugar que ocupa la tecnología* para la comisión del delito *más que a la naturaleza delictiva del acto mismo. "Si una persona intimida o intenta chantajear a otra persona vía correo electrónico, el dispositivo informático actúa como medio para cometer el hecho ilícito, siendo el delito de amenaza el hecho ilícito en sí. En el segundo caso, el dispositivo informático es el objeto o blanco del crimen, donde una persona puede enviar un virus a la computadora de un tercero y así dañarla a los fines de inutilizarla o alterar su funcionamiento. En este último caso la figura delictiva podría encuadrarse dentro del daño en tanto delito contra la propiedad, considerando el dispositivo informático como un bien tangible, tanto así como la información que puede almacenar".*[10]

Por la definición anterior cabe señalar que si bien los delitos informáticos no se limitan a aquellos que se cometen en la nube, es a partir de la liberalización comercial a mediados de la década del 90 por parte del gobierno de los Estados Unidos y su posterior expansión global cuando estas conductas comienzan a adquirir una nueva dimensión al respecto. Internet es una *red global de dispositivos informáticos* -computadoras, teléfonos móviles, tabletas, consolas de juegos, entre otros- que permite enviar, recibir y transmitir datos e información mediante el uso de un protocolo común de comunicaciones[11]. La crea el Departamento de Defensa de ese país en plena Guerra Fría con una finalidad puramente militar, la de crear un medio de comunicación alternativo al sistema de telecomunicaciones de ese país frente a un posible ataque nuclear soviético que colapsara las comunicaciones en ese territorio[12]. En un inicio la mayoría de dispositivos conectados a la red eran computadoras, en la actualidad multiplicidad de aparatos tecnológicos o dispositivos de tipo informáticos tienen capacidad de conectarse a la misma. La palabra "dispositivo" hace alusión a un aparato o mecanismo capaz de ejecutar una o varias acciones con un fin determinado, mientras que el término "informática" es una conjunción de las palabras "información" y "automática" y refiere al procesamiento automático de la información mediante dispositivos electrónicos y sistemas de computación. De esta manera, un dispositivo informático es un aparato capaz de procesar en forma automática datos e información con un fin determinado.[13]

(9) A diferencia de los delincuentes comunes y profesionales, para Sutherland, el delito de cuello blanco es cometido por personas de respetabilidad y estatus social alto en el curso de su ocupación. Asimismo tiene la capacidad de generar temor y admiración en la gente por producir ingresos en forma ilícita sin ser alcanzados por la justicia

(10) Sain, Gustavo: "Internet, el cibercrimen y la investigación criminal de delitos informáticos". En Azzolin, H. y Sain, G.: "Delitos informáticos: investigación criminal, marco legal y peritaje" - BdeF - Bs. As. - 2017 - pág. 8

(11) El protocolo de comunicaciones de internet es el TCP/IP, siglas de *Transmission Control Protocol/Internet Protocol* (Protocolo de Transmisión de Internet/Protocolo de Internet)

(12) Leiner, Barry; Cerf, Vinton; Clark, David *(et al)*: *"A brief history of Internet"* - Internet Society - Washington - 2003

(13) Un dispositivo informático debe contar con la capacidad de desempeñar tres tareas básicas, a saber: la entrada, el procesamiento y la salida de información en forma electrónica. Así, computadoras personales (PC, notebooks, tablets), teléfonos celulares, cámaras fotográficas, filmadoras, televisores inteligentes, consolas de juegos, entre otros, entran en la categoría de dispositivos informáticos

En la actualidad, los delitos informáticos pueden clasificarse en dos grandes grupos: *aquellos que requieren de una sofisticación técnica para su comisión,* generalmente basado en la elaboración de programas maliciosos desarrollados por *hackers* que buscan vulnerar los dispositivos o redes, generalmente con fines económicos y *aquellos delitos que adquieren una nueva vida en la nube y son intermediados por servicios y aplicaciones web* como las amenazas, los fraudes, el *grooming*[14]. Muchos de ellos se cometen en lo que en informática se denomina "ingeniería social", que a diferencia de la ingeniería técnica basada en la elaboración de programas maliciosos apela al proceso de la comunicación para engañar a un usuario con una finalidad económica, sacarle dinero o producir lo que se denomina como suplantación de identidad, la obtención de datos personales o institucionales de terceros.

Luego hay otros tipos de *delitos vinculados a la violación de la privacidad de los personas* en tres niveles: *Las intervenciones ilícitas de los gobiernos por sobre las comunicaciones privadas de los ciudadanos,* como es el caso del espionaje ilegal de las agencias de inteligencia y seguridad de los Estados Unidos sobre ciudadanos extranjeros con programas de vigilancia en la lucha contra el terrorismo; *la violación a la intimidad por parte de las empresas proveedoras de servicios de internet en términos comerciales* sin el consentimiento del usuario para conocer sus gustos y preferencias y establecer la venta agresiva de productos y servicios asociados y *el uso de la informática en el ámbito laboral,* cuando en el marco de una organización empleadora se accede a comunicaciones privadas de un trabajador (mails, redes sociales, etc.) y lo despide del trabajo.

Desde un punto de vista criminológico, en la actualidad no existe una rama o área de estudio que aborde esta problemática desde esta perspectiva. Algunas disciplinas que se ocupan de esta temática son, por un lado, el *Derecho* y, por otro, el campo de la *seguridad informática*, que entiende acerca de cuestiones relacionadas con la seguridad de los dispositivos computacionales desde un punto de vista tecnológico.

III - DERECHO Y NUEVAS TECNOLOGÍAS

Derecho e informática

Para Manuel Castells, un nuevo paradigma tecnológico surgido durante la década del 70, en Estados Unidos, dio lugar a un nuevo modelo de desarrollo basado en las tecnologías de la información, que sustituirá al modelo industrialista vigente en las sociedades modernas desde la revolución industrial del siglo XIX. La innovación tecnológica y el cambio organizativo, centrados en la flexibilidad y la adaptabilidad, resultaron condicionantes para la reestructuración del sistema capitalista. Es cuando durante la década del 80 entró en vigor *un nuevo modelo de desarrollo: el informacionista.* El cual destaca el papel de la información dentro de la sociedad. La sociedad informacional, para Castells, indica una forma de organización social en la que la generación, procesamiento y transmisión de información son factores fundamentales en términos de productividad y poder. En este sentido, la revolución de las tecnologías de la información produce a nivel global un nuevo modo de producir, comunicar, gestionar y vivir.[15]

(14) El *grooming* es un acoso sexual cometido por un pedófilo a un niño, niña o adolescente mediante el uso de servicios y aplicaciones de internet con el objetivo de abusar sexualmente de él

(15) Castells, Manuel: "Prólogo: la red y el yo", en "La era de la información: economía, sociedad y cultura" - Siglo XXI Editores - México D.F. - 2001

Con la llegada de la informática, el derecho tuvo que adaptar su teoría no solo para la protección de los datos y la información digitales como bienes jurídicos sino también para el uso de los dispositivos automatizados para el mejoramiento de procesos administrativos. Así, tras el surgimiento de la cibernética[16] en 1949, como nuevo campo de estudio, el jurista estadounidense Lee Loevigner publica ese mismo año un artículo -bajo el título *"Jurimetría, el próximo paso"*- donde analiza la aplicación de recursos informáticos para el tratamiento de la *información jurídica*. La informática jurídica representa el primer campo de relación entre el derecho y la tecnología, y refiere a la aplicación de dispositivos informáticos para el tratamiento de la información legal[17]. En cuanto a la protección de bienes jurídicos, existe un área relacionada con el derecho penal abocado al estudio de aquellos ilícitos donde la tecnología informática desempeña un papel condicionante. Es a través del *derecho informático* o *derecho de alta tecnología* en donde se aplican las reglas jurídicas con los problemas vinculados con la tecnología.[18]

Históricamente, diferentes bienes inmateriales o intangibles fueron considerados por las legislaciones penales como un bien jurídico a proteger. Así sucedió con la materia y la energía, contempladas en los códigos modernos de occidente. Como se describe en el Manual de las Naciones Unidas sobre Prevención y Control de Delitos Informáticos de 1994:

> *"Hasta ahora, los códigos penales de todos los países se ha protegido de forma preponderante a los objetos tangibles y visibles. Aunque la protección de la información y de otros objetos o valores intangibles existía ya a mediados del siglo XX, lo cierto es que hasta muy recientemente no ha revestido importancia. En los últimos decenios se han producido cambios importantes: de una sociedad industrial se ha pasado a una sociedad posindustrial, el valor de la información ha aumentado en las esferas económica, cultural y política, y se ha incrementado la importancia de la tecnología informática, cambios que han planteado nuevos problemas jurídicos y han requerido nuevas respuestas jurídicas a la legislación en materia de información".*[19]

Entendidos como *delitos informáticos, cibercrimen, delitos cibernéticos* o *delitos de alta tecnología,* entre otros términos, los diferentes países comenzaron a modernizar su legislación de acuerdo con estas nuevas modalidades ilícitas de tres maneras: 1. En un principio, algunos Estados intentaron aplicar figuras típicas convencionales para la

(16) En 1948, el matemático estadounidense Norbert Wienner, en su libro "Cibernética o el control y comunicación en animales y máquinas", habla de una nueva disciplina para la organización de la sociedad sobre la base de una nueva materia prima: la información. Esta, junto a las máquinas y las redes, debía actuar en contra de la entropía, la tendencia natural a precipitar la degradación biológica y el desorden social

(17) Si bien es una disciplina que se encuentra dentro del campo de las ciencias de la información, es puesta al servicio del derecho para la compilación y búsqueda de documentos jurídicos (informática jurídica documental); como ayuda a los procesos jurídico-administrativos tradicionales (informática jurídica administrativa o de gestión) y aquella que busca suplantar decisiones humanas mediante el uso de programas automatizados de *software* (informática jurídica decisional)

(18) Sain, Gustavo: "La informática jurídica, el derecho informático y el cibercrimen" - Ed. Rubinzal-Culzoni Editores online - marzo/2017

(19) Organización de las Naciones Unidas (ONU): "Manual de las Naciones Unidas sobre prevención y el control de delitos informáticos" - Revista Internacional de Política Criminal - Naciones Unidas - Nos. 43 y 44 - Nueva York - 1994

protección de los datos e información digital y los dispositivos informáticos, como, por ejemplo, los delitos contra la propiedad. Cuando el bien afectado era la computadora personal; o los delitos contra la intimidad, para el caso de la interceptación del correo electrónico como correspondencia personal. 2. Otros, sin embargo, modificaron sus leyes para incorporar nuevas figuras que incluyan a la información como un bien jurídico a proteger, como sucedió con las leyes de propiedad intelectual, redactadas para la protección de los derechos de autor de obras literarias, científicas, musicales y cinematográficas en el mundo físico. En estos casos, se actualizaron sus contenidos para incorporar a los programas de computación y aplicaciones de *software*. 3. Por último, ya en la actualidad muchos países incorporaron los delitos informáticos a su normativa, mediante la promulgación de leyes específicas en el área, entendidas como "leyes de delitos informáticos".[20]

Para el jurista alemán Ulrich Sieber, históricamente hubo diferentes oleadas de reforma legislativa en la materia, tal como lo señala en un informe titulado *"Aspectos jurídicos de la delincuencia informática en la Sociedad de la Información"*, presentado ante las autoridades de la Unión Europea en 1998. Para este autor, los procesos de reformas se inician a partir de la década del 70 con el objeto de proteger la privacidad de los datos a partir de las nuevas formas de recolección, almacenamiento y transmisión de información a través de sistemas informáticos. Países como Suecia (1973), Estados Unidos (1974) y Alemania (1977) incorporaron figuras en sus legislaciones relacionadas con la protección de los datos personales. La segunda oleada comienza en la década del 80 con la protección que establecen los países europeos de bienes inmateriales frente a la aparición de sistemas de pago electrónico, proceso que fue iniciado por los Estados Unidos en 1978.

El tercer campo está relacionado con la protección de la propiedad intelectual, donde diversos países establecieron reformas a las leyes de patentes promulgadas durante los años setenta para evitar la reproducción y venta no autorizada de obras digitales. Países como Estados Unidos (1984), Japón (1985) y Suecia (1986), entre otros, establecieron legislaciones específicas para la protección de obras en semiconductores y chips. La cuarta tendencia reformista, por su parte, estuvo relacionada con los contenidos ilícitos y nocivos tales como la difusión de pornografía infantil, la llamada incitación al odio o la difamación. Mediante la adaptación de las leyes tradicionales a las nuevas tecnologías, Gran Bretaña (1994) y Alemania (1997) iniciaron el proceso, tanto así como el establecimiento de responsabilidad de los proveedores de servicio y acceso a internet sobre el material publicado, en Estados Unidos (1996) y Alemania (1997). Por último, la última oleada de reformas se dio en materia de derecho procesal penal iniciado en Australia (1971), en Gran Bretaña (1984), Dinamarca (1985) y Estados Unidos (1986), entre otros.[21]

Armonización penal y cooperación internacional

La Organización Internacional de Policía Criminal (Interpol) realizó en 1979 una conferencia internacional, en París (Francia), donde se expresaba que *"la naturaleza de los delitos informáticos es internacional debido al incremento de las comunicaciones telefónicas, satelitales, etc. entre diferentes países. Las organizaciones internacionales deben*

(20) Sain, Gustavo: "Dificultades del proceso judicial en la investigación de delitos relacionados con dispositivos informáticos", en Azzolin, Horacio y Sain, Gustavo: "Delitos informáticos: investigación criminal, marco legal y peritaje" - BdeF - Bs. As. - 2017

(21) Sieber, Ulrich: "El problema: tipos comunes de delitos informáticos". En Aspectos legales de los delitos informáticos en la sociedad de la información. Bruselas, Informe de la Comisión Europea - 1998

prestar más atención en este aspecto"[22]. Desde la década del 80, existen diferentes documentos de referencia elaborados por organismos internacionales que intentaron armonizar las legislaciones de los países a partir de una serie de recomendaciones en materia penal y procesal penal para la persecución de este tipo de conductas.

En este sentido, la Organización para la Cooperación y el Desarrollo Económico (OCDE) convocó en 1982 a un grupo de expertos con el fin de ajustar la legislación penal de los países miembros para la protección de programas y sistemas informáticos ante el temor al uso indebido de las redes informáticas y su repercusión en la economía de las naciones. Como corolario de la misma, en 1986, el organismo publicó un informe titulado *"Computer related crime: analysis of the legal policy"* ("Delitos de informática: análisis de la normativa jurídica") con una lista mínima de ejemplos sobre delitos informáticos a modo de propuesta para la actualización de los códigos de los países miembros.

El Consejo de Europa elaboró en 1989 una serie de directrices orientadas a los parlamentos de los países miembros en relación con los tipos de conductas punibles donde intervenían dispositivos informáticos. Mediante la conformación de un Comité Especial de Expertos sobre Delitos Relacionados con el Empleo de Computadora se abordaron temas como la prevención de riesgos, represión de este tipo de delitos, procedimientos de investigación, métodos de confiscación internacional, y cooperación internacional.

Un año más tarde fue el turno de la Organización de las Naciones Unidas que, tras la realización del Octavo Congreso sobre la Prevención del Delito y Tratamiento del Delincuente celebrado en La Habana (Cuba), incorporó a su agenda el tema, producto de un mayor empleo de las tecnologías de la información en las economías y burocracias de los países, señalando por primera vez el uso que podía hacer el crimen organizado de las tecnologías de la información y la red internet. Según el documento final, *"la delincuencia organizada puede utilizar dichas técnicas para fines tales como el blanqueo de dinero o para la gestión y transferencia de activos adquiridos ilegalmente"*.[23]

Tras la realización del congreso, el gobierno de Canadá se ofreció a elaborar un manual que contenga una serie de normas y directrices en materia de seguridad informática. Luego de la realización de un coloquio sobre delitos, organizada por la Asociación Internacional de Derecho Penal, en 1992, en Wurzburgo (Alemania), se publica, dos años después, el *Manual de las Naciones Unidas sobre Prevención y el Control de Delitos informáticos* de 1994, donde se identifica las diferentes modalidades ilícitas cometidas mediante el uso de computadoras.

Por último, en el año 2001, se firma en Budapest (Hungría) el *Convenio sobre la ciberdelincuencia* en el seno del Consejo de Europa ante la necesidad de *"prevenir los actos que pongan en peligro la confidencialidad, la integridad y la disponibilidad de los sistemas, redes y datos informáticos..."*[24]. El Convenio establece diferentes tipologías del delito en el ámbito de la cibercriminalidad como modelo legislativo, tanto en el ámbito de derecho penal como procesal penal; principios generales de cooperación entre los diferentes países en materia judicial y procedimientos vinculados a la investigación criminal.

(22) Schjolberg, Stein: "*The history of global harmonization on cybercrime legislation. Road to Geneva*" - Documento web - pág. 8

(23) Organización de las Naciones Unidas (ONU): "Informe del Octavo Congreso sobre la Prevención del Delito y Tratamiento del Delincuente" - Secretaría General de Naciones Unidas - Nueva York - 2000 - pág. 149

(24) Consejo de Europa: "Convenio sobre la ciberdelincuencia" - Publicación del Consejo de Europa - Estrasburgo - 2001 - Preámbulo

Su entrada en vigencia se produjo el 1/7/2004, y a la fecha, más de 50 países se encuentran suscriptos a él, siendo el documento internacional de mayor referencia en la actualidad.[25]

Investigación criminal

Con la incorporación de dispositivos informáticos a la vida cotidiana de las personas, desde fines de los años setenta, ante la comisión de un delito, la criminalística tradicional tuvo que establecer nuevos tipos de peritajes para la obtención de evidencia de tipo electrónica. Así, a principios de los años ochenta, en Estados Unidos, surge una disciplina dentro del ámbito de la informática, la *informática forense.* Para el FBI, *"es la ciencia que se encarga de adquirir, preservar, recuperar y presentar datos que han sido procesados electrónicamente y guardados en un medio informático"*[26]. La evidencia digital está constituida por los datos e información que se almacena, trasmite o recibe en un dispositivo informático que tiene valor probatorio en el marco de una investigación judicial cuando las circunstancias de un acontecimiento permitan sospechar de la comisión de un delito. La evidencia digital, también entendida como prueba informática, es de naturaleza intangible, inmaterial, en tanto que constan de impulsos eléctricos procesados automáticamente por un dispositivo informático.[27]

La investigación criminal de ilícitos donde intervienen dispositivos informáticos presenta una serie de dificultades. En primer lugar, cabe señalar que una característica propia de los delitos informáticos es el *bajo índice de denuncia judicial*[28] a nivel global, lo que insume una amplia cifra oculta de este tipo de conductas. Existen varios factores que explican por qué, en este tipo de criminalidad, prácticamente, los gobiernos no tienen intervención:

1. *El desconocimiento de las personas que están siendo víctimas de un delito informático,* en tanto que muchos usuarios son víctimas de estas conductas sin tomar conocimiento de esta situación, como, por ejemplo, sucede ante la presencia de un archivo espía o *spyware* instalado en forma oculta en un dispositivo.
2. Por otro lado, existe también *el derrotero de los usuarios sobre una resolución efectiva en términos judiciales* de determinados tipos de delitos.
3. La no denuncia de incidentes informáticos producidos en el marco de una red interna de una organización privada por *el temor de las empresas privadas ante la posibilidad de ver afectada su imagen y reputación* y/o también evitar multas o sanciones penales o administrativas.
4. Por último, las *resoluciones técnicas y administrativas* de una gran cantidad de delitos, cuando, por ejemplo, ingresa un virus a una computadora y es detectado por un programa antivirus se elimina o cuando se *"hackea"* una casilla de correo y se utilizan los mecanismos de resolución brindados por las empresas proveedoras de servicio de internet, permiten recuperar la cuenta a su legítimo usuario.

(25) Otros organismos que abordaron la problemática de la criminalidad informática son el G-8, la Unión Internacional de Telecomunicaciones (UIT) y The Commonwealth, entre otros

(26) Noblett, Michael; Pollitt, Mark y Presley, Lawrence: "Recuperación y examen de evidencia en informática forense". En Revista Ciencias de la comunicación forense. Washington, publicación de la Oficina Federal de Investigación (FBI) 2000, N° 4 - vol. 2 - pág. 1

(27) Sain, Gustavo: "Internet, el cibercrimen y la investigación criminal de delitos informáticos", en Azzolin, Horacio y Sain, Gustavo: "Delitos informáticos: investigación criminal, marco legal y peritaje" - BdeF - Bs. As. - 2017 - pág. 8

Otro factor que hace a la dificultad de investigación criminal de delitos en los que interviene un dispositivo informático es la *fragilidad de la prueba informática.* En estos tipos de delitos, el lugar del hecho donde se encuentran los potenciales elementos probatorios es un *entorno virtual.* Que sea virtual no implica que no tenga existencia real, pero los entornos digitales simulan ser representaciones de objetos físicos, para lo cual la escena del crimen, además de física, es lógica. Por otro lado. la evidencia digital es *flexible*, ya que los archivos digitales se pueden suprimir o alterar en forma muy sencilla; es *volátil*, porque la existencia de cierta información digital depende de la energía eléctrica y puede perderse automáticamente al apagar o desenchufar un dispositivo; es fácilmente *ocultable*, ya que puede estar guardada en dispositivos de almacenamiento externos -tales como CD, DVD, pendrives, discos rígidos externos, etc.-, carpetas ocultas, servidores extranjeros, y puede estar codificada, almacenada en formatos especiales, dentro de otros archivos o almacenada con nombres falsos, entre otros. Por último, la prueba informática puede ser *anónima*, en tanto que los archivos digitales no imprimen rasgos personales de sus usuarios. En este último punto, la ausencia de indicios de identidad en las comunicaciones de internet dificulta la identificación de responsables de los hechos. En la internet comercial, el uso de los servicios y aplicaciones más populares de la red -Facebook, YouTube, WhatsApp, Twitter, Google, entre otros- es gratuito, ya que la fuente principal de sus ingresos es la publicidad. En este sentido, el objetivo de los proveedores no está puesto en la identificación de la persona que se encuentra detrás de la pantalla, sino en sus gustos y preferencias. De esta manera, internet favorece la construcción de identidades ficticias ante la ausencia de mecanismos de acreditación de identidad certeros por parte de las empresas proveedoras de servicios.[29]

Un tercer factor que hace a los procesos de investigación judiciales de delitos informáticos es el conflicto existente en términos de jurisdicción y territorialidad, si se comete en la nube. Un delito que se comete en internet puede realizarse desde un dispositivo y afectar a otros alrededor del mundo -como sucede con la distribución de virus, por ejemplo-. Asimismo, por más que se limite a un solo país en cuanto a usuarios afectados, los datos y la información que circulan a través de las redes atraviesan diferentes computadoras "ruteadoras" y se almacenan en servidores en el extranjero, de acuerdo con el servicio o aplicación web que sea utilizado para su distribución. En estos casos y en otros delitos de tipo convencional, se debe recurrir a las empresas proveedoras de servicio que almacenan registros de comunicaciones y datos de los usuarios. Por ello, ante una denuncia radicada en un determinado país, en la actualidad, existen inconvenientes en términos de solicitudes cursadas por los tribunales de un país, fundamentalmente cuando la empresa es multinacional. Ante la requisitoria de la justicia local, la misma puede negarse a brindar la información bajo los siguientes argumentos:

(28) De acuerdo con el informe *"Una aproximación a la estadística criminal sobre delitos informáticos: primer muestreo de denuncias judiciales de la República Argentina"* realizado por la Dirección Nacional de Política Criminal en materia de Justicia y Legislación Penal del Ministerio de Justicia y Derechos Humanos de la Nación, de un total de 46.043 causas judiciales, que se tramitaron en los tribunales de todo el país en el año 2013, 221 presentaciones involucraron alguna de las figuras penales de la L. 26388 o "ley de delitos informáticos", lo que representa un 0,48% del total. En términos del fuero criminal y correccional de la Provincia de Buenos Aires, durante ese mismo año, de 694.246 denuncias, solo 275 causas se relacionaron con dicha normativa, ocupando solo un 0,04% del total

(29) Sain, Gustavo: "Internet, el cibercrimen y la investigación criminal de delitos informáticos", en Azzolin, H. y Sain, Gustavo: "Delitos informáticos: investigación criminal, marco legal y peritaje" - BdeF - Bs. As. - 2017 - pág. 8

- *La empresa no tiene representación legal en el país,* por lo cual la solicitud se debe cursar mediante exhorto al país donde figure su sede legal.
- El proveedor de servicios tiene representación legal en el país, pero *sus servidores se encuentran en el extranjero* y debe realizar la requisitoria en ese país.
- La empresa posee una sede física y legal en el país y la información requerida se encuentra almacenada en servidores locales, pero al ser una empresa extranjera *se rige con la legislación de privacidad de los datos de ese país* y no puede brindar esa información.(30)

Asimismo, *internet no posee un organismo central que permita centralizar las requisitorias de información en términos judiciales* en tanto que la misma es administrada por un conjunto de organizaciones sin fines de lucro que se encargan de fijar políticas técnicas. Bajo el modelo *multi stakeholder* o "de partes interesadas", empresas del sector de telecomunicaciones e informática, organismos no gubernamentales, instituciones académicas y organismos de gobierno de diferentes países establecen, en forma no vinculante, los estándares tecnológicos y los protocolos de comunicación generales para el funcionamiento de la red. En este sentido, la organización más importante es la Corporación de Internet para la Asignación de Nombres y Números -ICANN, por sus siglas en inglés-, fundada en 1998, es la encargada de asignar las diferentes direcciones web, aplicar los protocolos aprobados públicamente y administrar los servidores que realizan el transporte de los datos en las comunicaciones.

IV - LA SEGURIDAD INFORMÁTICA COMO ESTRATEGIA TÉCNICA

Orígenes de la seguridad en las organizaciones

El origen de la seguridad en las organizaciones surge a principios de siglo XX con el objetivo de proteger las instalaciones físicas frente a los conflictos sociales y laborales de la época. Al igual que con la legislación penal, estaba orientada a salvaguardar las propiedades y personas, en este caso específicamente contra el robo, fuego, inundación, contrarrestar huelgas y felonías y, de forma amplia, todos los disturbios sociales que puedan poner en peligro el progreso e incluso la vida del negocio.

En cuanto a la seguridad informática, un hecho que puede representar el inicio de este campo como forma de abordaje a la problemática del cibercrimen sucede en 1988 en Estados Unidos, donde un estudiante de 23 años de la Universidad de Cornell, Robert Tappan Morris, propagó un programa capaz de replicarse automáticamente con el objetivo de medir el tamaño de ARPANET -nombre que recibía internet por aquel entonces-. Un supuesto error de programación hizo que se replicara en forma indiscriminada por la toda la red, y ante la imposibilidad de eliminarse, infectó al 10% de los equipos conectados a la red (unas 6.000 computadoras). Tal fue el impacto del mismo que el jueves 3/11/1988 es conocido en la historia de la informática como *Black Thursday* -término utilizado para los cracs bursátiles-.

En términos técnicos, el caso tomó repercusión no solo por los efectos producidos sino por la complejidad del diseño del gusano, tanto así como por la facilidad y rapidez en propagarse. Computadoras de puntos vitales tales como la NASA, la RAND, el Pentágono,

(30) Sain, Gustavo: "La informática jurídica, el derecho informático y el cibercrimen" - Ed. Rubinzal-Culzoni Editores online - marzo/2017

las Universidades de Berkeley, Princeton y Stanford, el MIT e incluso la MILNET -la red militar que nucleaba organismos de las fuerzas armadas de los Estados Unidos- fueron cayendo una tras otra a partir de los efectos del programa malicioso. En términos económicos, se estima que la desinfección del gusano en las computadoras afectadas tuvo un costo de aproximadamente 10 millones de dólares de acuerdo con las estimaciones de gastos de universidades, laboratorios de investigación privados y organismos militares que fueron afectados por Morris.[31]

Ante las cuantiosas pérdidas económicas en universidades, el ejército y el sector privado, el gobierno de los Estados Unidos decide crear el Equipo de Respuestas ante Emergencias Informáticas (CERT, *Computer Emergency Response Team*), que opera hoy en día como el organismo central del país en términos de seguridad informática.

El campo de la seguridad informática

La *seguridad informática* es entendida como cualquier acción que impida la ejecución de operaciones no autorizadas sobre un sistema informático o red de computadoras. En líneas generales, comprende el conjunto de medidas preventivas, de detección y corrección destinadas a proteger los recursos informáticos de una organización.

Existe una figura por la que se suele explicar los alcances de este campo, aquella que suele conocerse como la tríada CIA, en alusión a las iniciales de las palabras en inglés *Confidenciality, Integrity y Availability. La confidencialidad, la autenticidad y la integridad* aluden a tres propiedades que poseen los datos y la información almacenados, transmitidos o recibidos en dispositivos informáticos. La confidencialidad representa la garantía de que cada mensaje transmitido por las redes pueda ser leído por su legítimo destinatario, la autenticidad a la legitimidad de la identidad del creador de un mensaje. Mientras que la integridad se relaciona con la garantía de que los contenidos de un documento no hayan sido alterados desde su creación o durante su transmisión en red.

Para Álvaro Gómez Vieytes, el objetivo de la seguridad informática es la de mitigar los efectos de las amenazas y vulnerabilidades mediante una serie de *controles preventivos, disuasivos, detectivos, correctivos y recuperativos.* Los controles preventivos y disuasivos se realizan antes de que se produzca un incidente de seguridad, con el objetivo de evitarlo. Los controles detectivos, como su palabra lo indica, buscan detectar un incidente informático cuando se están produciendo, mientras que los controles correctivos y recuperativos se desarrollan una vez producido el mismo con la finalidad de resguardar un sistema informático de los daños y la información que almacena.

(31) Lo llamativo del caso es que el padre de Morris, Robert, era científico del Centro Nacional de Seguridad Informática de la Agencia de Seguridad de los Estados Unidos. Este es quien termina convenciéndolo de que confiese a cambio de una reducción de la pena. De esa manera, Robert Morris Jr. solo fue condenado en 1990 a 3 años de libertad condicional, una multa de 10.000 dólares y 400 horas de servicio comunitario, siendo el primero por la cual se aplicó la ley de fraude y abuso de computadoras de los Estados Unidos de 1986. Al igual que otros casos, Morris adquirió popularidad dentro de la comunidad *hacker*, donde figura como algunos de sus logros la creación de Viaweb -una de las primeras plataformas de comercio electrónico- quien vendió a Yahoo! por 48 millones de dólares -hoy Yahoo! Store-, la creación de la empresa Y Combinator y la participación en la elaboración de lenguajes de programación. Asimismo desarrolló una carrera docente como profesor del MIT

Asimismo, la seguridad informática no solo es lógica, sino que también posee *controles de tipo físicos, técnicos y administrativos.* Los primeros incluyen medidas de protección física (cerraduras electrónicas, sistemas de acceso biométrico, cámaras de seguridad, etc.), mientras que los técnicos o lógicos son aquellas medidas abocadas a la seguridad de las aplicaciones y del sistema operativo de un dispositivo, ya que incluyen a los programas de *software*. Por último, están los controles administrativos, que son aquellos que hacen a la política de seguridad de una organización.

Algunos conceptos que son centrales en este proceso y resultan importantes en el campo de la seguridad informática son: *recursos del sistema, amenazas, vulnerabilidad, incidente de seguridad, impacto y riesgo. Los recursos del sistema* refieren, básicamente, a los recursos que debe proteger la organización, entre los que figuran: *los elementos de hardware*, como, por ejemplo, las computadoras, impresoras y escáneres; y *los programas de software*, los sistemas operativos, los programas de gestión y herramientas de programación, entre otros. Entre los activos de una organización a proteger se incluyen: *los elementos de comunicaciones* como el cableado, los puntos de acceso a la red, y las líneas de comunicaciones, entre otros; *los locales y oficinas; las personas* que utilizan y se benefician del sistema; y *la imagen y reputación de la organización.*

Por *amenaza informática* se entiende a los eventos accidentales o intencionados que puede ocasionar algún daño a un sistema informático y ocasionar pérdidas materiales o financieras a la organización. Existen diferentes tipos de amenazas: naturales (incendios, inundación, tormenta, fallas eléctricas, explosiones, etc.); agentes externos (ataques de una organización criminal, sabotajes, disturbios y conflictos sociales, robos, estafas, virus informáticos, etc.) y agentes internos (descuidos del personal, errores involuntarios en el manejo de herramientas, sabotaje por parte de empleados descontentos, entre otras).

Una *vulnerabilidad informática* es una debilidad que presenta un sistema informático que puede permitir que las amenazas causen daños en los mismos. Un *incidente de seguridad*, por su parte, puede ser definido como un evento que puede producir una interrupción de los servicios brindados por un sistema informático, causando así pérdidas materiales o financieras a la organización. En cuanto al *impacto*, el mismo refiere a la medición y valoración de un daño que podría producirse en una organización un incidente de seguridad. Por su parte, el *riesgo* es la probabilidad de que una amenaza se materialice sobre una vulnerabilidad del sistema informático, causando un determinado impacto en la organización.[32]

Por último, existen tres conceptos fundamentales en términos de seguridad informática, los mismos son los de *políticas, planes y procedimientos*. Una política de seguridad de una organización comprende los principios y líneas de acción básicos que hacen a la seguridad de los sistemas informáticos, incluyendo las responsabilidades del personal en las cuestiones técnicas y organizativas. El plan de seguridad de la organización

(32) Otra dimensión de la seguridad informática es la seguridad física de las instalaciones, básicamente la seguridad de los lugares donde se ubican los dispositivos informáticos en una organización. Incluyen medidas como la protección frente a incendios, explosiones, inundaciones, accesos no autorizados, etc.; la selección de elementos de construcción internos tales como puertas, ventanas, paredes, suelos y techos, centrales eléctricas, elementos de comunicaciones etc.; y la definición de áreas dentro de la organización, tales como áreas públicas, áreas con acceso restringido, etc., entre otras

incluye al conjunto de decisiones que definen las acciones futuras y los medios a utilizar para tal fin, mientras que los procedimientos son las tareas y operaciones a ejecutar de acuerdo con las políticas de seguridad.[33]

La seguridad de las redes informáticas de un país

Como se señaló anteriormente, los organismos centrales en materia de seguridad informática a nivel de un país o región están representados por un Equipo de Respuestas ante Emergencias Teleinformáticas (*Computer Emergency Response Team* - CERT)[34], modelo surgido en Estados Unidos a fines de la década del 80 a partir de la distribución del primer *software* malicioso de la historia de internet, el Gusano Morris. Ante las cuantiosas pérdidas económicas en universidades, ejército y sector privado, el gobierno decidió crear esta organización. Bajo la dirección de la Agencia de Proyectos de Investigación Avanzados del Departamento de Defensa de ese país (DARPA) consta de un centro de respuestas llevadas a cabo por un equipo de expertos en seguridad informática encargados de brindar medidas preventivas y reactivas a incidentes de seguridad en el marco de las organizaciones. En líneas generales, los CERT estudian el estado global de los sistemas y redes informáticas y ofrece servicios de apoyo -a modo de mesa de ayuda de una organización- frente a ataques de seguridad informática, publican alertas de amenazas y vulnerabilidades, y brindan información para mejorar la seguridad de los sistemas.

Las funciones principales de los CERT son:

- Ayudar al público a prevenir y atenuar incidentes en materia de seguridad informática.
- Proteger la integridad, confidencialidad y autenticidad de los datos e información digitales.
- Coordinar respuestas en forma centralizada frente a amenazas informáticas.
- Guardar evidencias por si los casos llegan a la justicia.
- Prestar asistencia a usuarios para la recuperación de los sistemas frente a un ataque informático.

  En cuanto a los servicios ofrecidos se destacan:

  - *Servicios preventivos:*
    - Avisos de seguridad.
    - Búsqueda de vulnerabilidades.
    - Auditorías o evaluaciones de seguridad.
    - Configuración y mantenimiento de herramientas de seguridad, aplicaciones e infraestructuras.

(33) Gómez Vieites, Álvaro: "Principios de la seguridad informática" - Enciclopedia de la Seguridad Informática - Alfaomega Grupo Editor - México D.F. - 2011

(34) En Europa se denominan CSIRT -*Computer Security Incident Response Team*, Equipo de Respuestas ante Incidencias de Seguridad Informáticas- ya que el nombre CERT se encuentra registrado por el Gobierno de los Estados Unidos por CERT Coordination Center (CERT/CC). La coordinación de los CSIRT está dado por el Foro de Equipos de Seguridad y Respuesta de Incidentes (*FIRST - Forum of Incident Response and Security Teams*), como asociación global. La coordinación de los CERT está dada por el CERT *Coordinacion Center* (CERT/CC) creado en 1998 en el seno del Instituto de Ingeniería del Software (SEI - *Software Engineering Institute*) de la Universidad Carnegie Mellon

- Desarrollo de aplicaciones de seguridad.
- Divulgación de información relacionada con seguridad informática.

- *Servicios reactivos:*
  - Gestión de incidentes de seguridad (análisis, respuesta y coordinación de incidentes de seguridad).
  - Gestión de vulnerabilidades (análisis, respuesta y coordinación de vulnerabilidades detectadas).

Los CERT, a su vez, tienen "socios", tales como los describe la organización entre los que figuran, en su mayoría, organismos gubernamentales -de seguridad y defensa, principalmente-, empresas -de computación e informática y de servicios públicos-, bancos y entidades financieras e instituciones educativas, entre otros. En cuanto a las vulnerabilidades, las mismas pueden ser reportadas tanto por personas particulares como por organizaciones. El principio básico de funcionamiento organizacional se basa en que el resguardo de la integridad de la información es responsabilidad del organismo que la genera o administra. Asimismo, la investigación del origen de los ataques y de quiénes son sus responsables corresponde a las autoridades de cada organismo que haya sufrido el incidente de seguridad, mientras que la reparación de las consecuencias de los incidentes que afectan recursos específicos será responsabilidad del organismo objeto del incidente. Una vez solucionado el mismo, el CERT elabora un informe público externo juntamente con los proveedores para abordar el incidente antes de armar un "informe público".(35)

Hasta el año 2001, los CERT aplicaban la lógica empresarial de implementación de acuerdos o convenios de confidencialidad en cuanto a la información que manejan. En líneas generales, desarrollan una política de no revelación de vulnerabilidades basada en los siguientes pasos: el CERT recibe una notificación acerca de una vulnerabilidad por parte de un socio; la verifica; establece comunicación con el proveedor; y cuando la misma es solucionada, es informada al resto de la comunidad. A partir de ese año, existe una política de revelación parcial de vulnerabilidades, donde el proveedor, una vez notificado del inconveniente, tiene 45 días para publicar la vulnerabilidad, período que puede ser extendido.(36)

(35) Documentación extraída del sitio web del CS*IRT* de los Estados Unidos

(36) En base a esta operatoria, el CERT de los Estados Unidos promueve el desarrollo de herramientas, métodos y productos para ayudar a las organizaciones, la realización de exámenes forenses y el monitoreo de redes. Produce artículos, informes técnicos y documentación respecto a la *expertise* de sus miembros. Las organizaciones pueden elegir entre varios modelos de seguridad, después de evaluaciones, entre lo que figuran: identificar fallos de seguridad, mejorar la resiliencia y medir el nivel de amenazas internas. Posee un área de inteligencia digital e investigación donde se presta colaboración con las agencias federales de seguridad y en cuanto a apoyo operacional, identificación de herramientas de desarrollo para agujeros de seguridad de *software* comercial. En este sentido, en 2003, mediante un acuerdo entre la Universidad Carnegie Mellon y el Departamento de Seguridad Nacional (DHS) se crea el US-CERT, el equipo nacional de respuesta a incidentes de seguridad informática. Si bien el CERT/CC y el US-CERT son organizaciones distintas, se encuentran relacionadas y trabajan juntamente con el mismo equipo de profesionales del CERT. A partir de allí, el CERT/CC aborda los casos de seguridad informática a nivel global, mientras que el US-CERT lo hace a nivel de seguridad nacional de los Estados Unidos

En Argentina, el órgano gubernamental dependiente de la Administración Pública Nacional certificado por el CERT de los Estados Unidos es el Programa Nacional de Infraestructuras Críticas de Información (ICIC). Creado en 2011, tiene como objetivo proteger los activos críticos de información de la Nación mediante la protección de las infraestructuras críticas del Sector Público Nacional, organismos interjurisdiccionales y organizaciones privadas o públicas que así lo requieran. Es un organismo de gobierno dependiente de la Jefatura de Gabinete de Ministros de la Nación. Hasta ese año, el programa se llamaba ArCERT -Coordinación de Emergencias en Redes Teleinformáticas- y era dependiente de la Subsecretaría de Tecnologías de Gestión de la Secretaría de Gestión Pública de la Jefatura de Gabinete de Ministros.

Las acciones que desempeña el ICIC son las de prevención, detección, respuesta y recupero tras un ataque informático a un sistema. Es un organismo certificado por el CERT, elabora reportes periódicos de incidentes de seguridad para el sector público nacional y trata de brindar soluciones en forma organizada, además de brindar asesoramiento técnico. Posee un sistema de avisos donde se brinda información a los socios como panorama de amenazas, vulnerabilidades publicadas, herramientas de ataque o dispositivos para tal fin, medidas de seguridad y protección, etc. También ofrece un servicio de alertas y advertencias, donde se divulga información sobre ciberataques, alertas de intrusión, virus informáticos, etc. Por último, existe una coordinación de respuesta a incidentes que brinda seguridad de la información en las organizaciones en cooperación con los propietarios y proveedores de la parte afectada.

Al igual que el CERT, el procedimiento de actuación del ICIC frente a la solicitud de asistencia de una organización es la siguiente: el resguardo de la integridad de la información es responsabilidad del organismo que la genera o administra. La investigación del origen de los ataques y de quiénes son sus responsables corresponde a las autoridades de cada organismo que haya sufrido el incidente de seguridad. La reparación de las consecuencias de los incidentes que afectan recursos específicos de la Administración Pública Nacional será responsabilidad del organismo objeto del incidente. La información confidencial es manejada por el ICIC de acuerdo a las Políticas y Procedimientos para la Gestión de Incidentes del CERT y acuerdos de cooperación establecidos con otros CERT nacionales e internacionales a través de otorgamiento de *tickets* asignados con un número único e irrepetible. Asimismo posee un punto de contacto con las agencias de seguridad y el Ministerio Público Fiscal.[37]

V - HACIA UN ABORDAJE INTEGRAL EN MATERIA DE CIBERCRIMEN

A modo de síntesis, de acuerdo a lo visto hasta el momento podemos decir que existen dos grandes áreas que abordan la problemática del cibercrimen en términos prácticos; el Derecho y la seguridad informática. El ámbito del Derecho posee una *perspectiva sancionatoria*, interviene cuando el delito ya se ha consumado, siendo su función en términos de seguridad la conjuración y represión del delito. En materia de prevención criminal, *la solución penal no resulta contra-motivacional* a aquellas personas que deciden voluntariamente cometer un delito informático, ya que las altas probabilidades de una persecución penal eficaz es remota en la mayoría de los casos en términos de

(37) Documentación extraída del sitio web del Programa Nacional de Infraestructuras Críticas de la Información Ciberseguridad de la República Argentina

identificación del responsable de estas conductas, fundamentalmente a partir del uso de identidades ficticias y lugares de conexión públicos. Un hacker no está con el código penal en la mano antes de cometer un delito por Internet.

Asimismo, *la estrategia de armonización en materia penal y procesal penal* promulgada por el Consejo de Europa y otros organismos internacionales *no ha resultado efectiva* a la luz de los resultados. En primer lugar, en la actualidad existen variadas discusiones acerca de que conductas tienen que ser consideradas delito informático y cuáles no. Asimismo, lo que puede considerarse una conducta lesiva en un país no puede serlo para otro. Cada país tiene la potestad soberana para establecer su legislación penal respecto a sus realidades socioculturales predominantes, lo que no debería impedir la cooperación internacional para la persecución penal de este tipo de ilícitos. Por otro lado, si bien la mayoría de los países tienen legislación relacionada con este tipo de criminalidad, existen figuras típicas que no están tipificadas en forma uniforme. Asimismo, la uniformidad en materia de herramientas legales para investigación criminal resulta utópica, ya que la misma dependerá de los factores antes mencionados en cuanto a las tradiciones en término de la privacidad de las personas de un país, por un lado, y el tipo de relación que establezca la justicia de un país con las empresas proveedoras de servicio de internet multinacionales. En el primer caso, un país puede establecer como figura procesal la interceptación de las comunicaciones en línea, mientras que para otro esto puede representar una violación a la intimidad de sus ciudadanos. En segundo lugar, la obtención de evidencia digital por parte de la justicia de un país va a depender tanto de cuestiones como si la empresa posee representación legal en ese territorio o sus servidores dentro del mismo.

Por otro lado, los hechos ilícitos que involucran dispositivos informáticos que llevan los tribunales son ínfimos a partir de las resoluciones técnicas y administrativas que poseen estas conductas, lo que representa una *amplia cifra oculta en este tipo de criminalidad.* En la actualidad son las empresas de seguridad informática que elaboran programas de *software* comerciales y poseen una mayor intervención que los propios Estados en términos de protección de datos e información y dispositivos de sus clientes. *"La mayoría de las empresas de seguridad informática elaboran informes o reportes periódicos … Dichos informes son elaborados por los laboratorios de investigación de estas empresas en base a amenazas, vulnerabilidades, programas maliciosos circulantes y algunas modalidades delictivas conocidas en determinado país o región. Muchos de estos informes estadísticos son utilizados por agencias y organismos gubernamentales, incluso algunos de ellos los han adoptado como estadísticas oficiales"*(38). Por otro lado, muchos de estos delitos tienen resoluciones brindadas por las empresas proveedoras de servicio de Internet a partir de sus políticas de contenido. En la actualidad, la misma, como parte de los términos y condiciones generales de uso de sus productos, resultan más importantes que las propias legislaciones de los países. Así, por ejemplo ante un caso de amenazas, la existencia de sitios web con contenido discriminatorio, casos de *grooming*, por ejemplo, tienen resoluciones administrativas a partir de los mecanismos de denuncia que ofrecen estas empresas a los usuarios de los servicios. Así, una vez adoptadas las medidas como bloqueo de usuarios, baja de contenido multimedia (fotos, audios y videos) de los servidores, borrado de comentarios escritos de los sitios web, entre otros, la mayoría de los

(38) Dirección Nacional de Política Criminal en materia de Justicia y Legislación Penal del Ministerio de Justicia y DDHH de la Nación: "Segundo muestreo de denuncias judiciales de la República Argentina" - Sistema Argentino de Informática Jurídica (SAIJ) - Bs. As. - 2017 - págs. 8 y 9

usuarios no recurre a la justicia para la persecución penal de los responsables de estos hechos ilícitos. Lo mismo sucede con los delitos de tipo económico cometidos en línea, donde el usuario está más preocupado en recuperar el dinero perdido que radicar una denuncia judicial, como sucede por ejemplo en los casos que acceden a su cuenta bancaria en la red o cuando un tercero utiliza su tarjeta de crédito para realizar compras en línea mediante la suplantación de identidad. En ambos casos no salen del marco de las empresas en tanto que con una breve investigación interna se les devuelve el dinero ya que cuentan con un seguro para ello y los consideran como parte de la fuga de negocios.

Por último, y más importante, es el *bajo índice de resolución judicial* sobre este tipo de conductas ilícitas a partir de la casi inexistencia de sentencias condenatorias a los responsables de estos crímenes. En la República Argentina, según la estadística oficial de denuncias judiciales elaboradas por el Ministerio de Justicia y Derechos Humanos de la Nación, a nivel de justicia federal en todo el país, los ingresos relacionados con la ley 26388 o "ley de delitos informáticos" representan, entre los años 2013 y 2016, un 0,4% aproximadamente del total de denuncias ingresadas. En la Provincia de Buenos Aires en términos de justicia ordinaria, este porcentaje oscila entre el 0,10 y 0,20[39]. Los motivos pueden deberse a los señalados anteriormente que presenta la investigación criminal de los delitos que se cometen en la nube, a los que se suman el derrotero de los ciudadanos acerca de la percepción del accionar de la justicia ante estos delitos, la falta de conocimientos por parte de las autoridades responsables de la aplicación de la ley y la ausencia de convenios de extradición o cooperación judicial de los países abonan esta afirmación.

En cuanto al otro campo que aborda la temática, la *seguridad informática*, podemos decir que la misma posee una *mirada técnico-preventiva* acerca del fenómeno del cibercrimen. Se aboca a la protección de los dispositivos desde el punto de vista de la seguridad del *software* y el *hardware*, tratando de mitigar las amenazas (virus, gusanos y troyanos), vulnerabilidades de los programas, fallos de seguridad e incidentes informáticos de todo tipo. La misma *pone el acento en la seguridad de los datos y la información digital y los dispositivos informáticos más que la seguridad de las personas.* Este campo surge específicamente para evitar pérdidas económicas de los sistemas informáticos de las organizaciones más que los dispositivos de los usuarios particulares. En líneas generales cada país posee un organismo central que oficia como CERT certificado por los Estados Unidos que se encarga de brindar asesoramiento técnico a sus "socios" brindando recomendaciones técnicas y realizando ensayos de ataques a los dispositivos y redes para verificar la solidez de seguridad de los mismos. En Argentina existe el Programa Nacional de Infraestructuras Críticas de la Información y Ciberseguridad y depende de la Jefatura de Gabinete de Ministros. De acuerdo con el funcionamiento de los CERT centrales podemos concluir que desde la perspectiva de la seguridad informática, *la responsabilidad última de que una persona no sea víctima de un ciberdelito es del propio usuario.* Es así que a partir de una serie de recomendaciones de seguridad técnica, información sobre amenazas, divulgación de soluciones a incidentes, entre otros intenta concientizar a los usuarios acerca de un uso seguro y responsable de la tecnología. Si se establece una analogía con la seguridad ciudadana, es como un programa de seguridad publica basado en blindar las casas y departamentos de las personas con rejas, alarmas, cámaras y el Estado brinde recomendaciones de cómo hacerlo y haga pruebas de penetración para ver si esas medidas de seguridad son seguras.

(39) Ver Colección de estudios sobre cibercrimen en el sitio web del Sistema Argentino de Informática Jurídica (SAIJ) del Ministerio de Justicia y DDHH de la Nación de la República Argentina

Inspiradas en este campo, la mayoría de las legislaciones a nivel global tienden a proteger la seguridad de los datos y la información digital y los dispositivos informáticos, y no la seguridad de las personas, lo que en parte explica, en términos concretos, las resoluciones técnicas y administrativas de muchos de estos delitos. En este sentido, el Convenio de Cibercriminalidad de Budapest, del cual se inspiraron muchos países para actualizar sus legislaciones y actual documento de referencia a nivel internacional, resulta vetusto a la luz del avance tecnológico en lo que a tecnologías digitales se refiere. Prueba de ello lo brinda el hecho de que una de las principales figuras denunciadas en términos judiciales, en la actualidad, está representado por el *grooming*, figura que no aparece entre las recomendaciones brindadas en dicha convención. Los motivos se deben, por un lado, a que esa modalidad delictiva no posee una "resolución técnica", mientras que por otro, en la época cuando se firmó el tratado no existía la banda ancha y por ende, las redes sociales tal como se las conoce hoy en día a partir de la imposibilidad de transmisión de foto y videos de alta calidad a través de conexiones telefónicas.

En síntesis, a partir de la mayor resolución técnica y administrativa de los delitos de tipo informático, en la actualidad es el sector privado que posee un panorama más acabado acerca de hechos ilícitos que se cometen en la red o en los dispositivos de los usuarios que los propios gobiernos, inclusive, el sector privado tiene mayor intervención que el público en cuanto a políticas de seguridad.

Gobierno de internet

Como se señaló anteriormente, internet no posee en la actualidad un gobierno central ni es regulado por un organismo internacional que establezca políticas vinculantes en cuanto a su desarrollo técnico y mucho menos, político. En la actualidad, la red es administrada por una serie de organizaciones sin fines de lucro que establecen los parámetros de seguridad técnica y protocolos de comunicación de manera global y de forma no vinculante para un mejor funcionamiento de las redes. En términos de gobierno de la red, una primera iniciativa sucedió en 2003, donde la Organización de las Naciones Unidas reunió en Ginebra (Suiza) a los representantes de 153 países para la elaboración de un plan de acción para el desarrollo de la sociedad de la información del siglo XXI. En la primera reunión de la Cumbre Mundial de la Sociedad de la Información (CMSI) se establecieron los principios de lo que se denomina "la gobernanza de internet", donde el grupo solicita al Secretario General de las Naciones Unidas *"elaborar una definición de trabajo del gobierno de Internet"* e *"identificar las cuestiones de política pública que sean pertinentes para el gobierno de Internet"*[40], entre otras.

En la segunda parte de la cumbre, realizada en Túnez en 2005, el plan de acción establece claramente que *"la designación del organismo encargado de las cuestiones de política pública de Internet es el derecho soberano de los Estados. Estos tienen derechos y responsabilidades en lo que concierne las cuestiones de política pública que suscita internet en el plano Internacional"*[41] estableciendo el rol de los Estados para el desarrollo y funcionamiento de la red, aunque se especifique que el sector privado, la sociedad civil, las organizaciones intergubernamentales y los organismos internacionales deben desempeñar un papel importante para la definición de las mismas. Si bien estos principios

(40) Organización de las Naciones Unidas (ONU): "Declaración de Principios de Ginebra de la Cumbre Mundial de la Información" - Publicación de las Naciones Unidas - Ginebra - 2003 - pág. 15

(41) Organización de las Naciones Unidas (ONU): "Agenda de Túnez para la sociedad de la información" - Publicación de las Naciones Unidas - Ginebra - 2005 - pág. 12

sientan las bases para la intervención de los Estados, la mayoría de las medidas propuestas estaban orientadas a generar un entorno propicio de inversiones financieras y corregir las imperfecciones del mercado en aras de disminuir la brecha digital entre países. Así, en la declaración de principios de Ginebra se señala que *"los gobiernos deben intervenir, según proceda, para corregir los fallos de mercado, mantener una competencia leal, atraer inversiones, intensificar el desarrollo de infraestructura y aplicaciones de las TIC, aumentar al máximo los beneficios económicos y sociales y atender a las prioridades nacionales"*.(42)

Desde el anuncio de liberación de la red internet en 1995 por parte del gobierno norteamericano hasta el día de hoy, los principios vigentes dentro de estas asociaciones son meramente liberales en tanto que el servicio universal a nivel global debe estar garantizado por el mercado, mediante la inversión privada, la competencia y un marco regulatorio flexible. En este sentido, la intervención de los gobiernos debe ser mínima en términos de diseño de políticas públicas. El modelo es el de una internet abierta y descentralizada, libre de intervenciones de los gobiernos y a favor de una autorregulación entre los usuarios y proveedores de servicio. Bajo esta perspectiva, los usuarios son considerados consumidores más que ciudadanos sujetos a derechos, ya que el objetivo es la confianza que le puedan garantizar las empresas proveedoras de servicio para desenvolverse en un entorno seguro y confiable en la red, fundamentalmente para la realización de operaciones financieras bajo la modalidad de comercio electrónico(43). En este sentido, actualmente los diferentes intentos de regulación por parte de los Estados de los entornos virtuales son prejuzgados como un posible acto de censura por parte de estas organizaciones en tanto afectan la libertad de expresión de los usuarios. Si bien es cierto que ha habido intervenciones ilegales por parte de ciertos Estados en materia de espionaje político y comercial, esta falsa dicotomía "libertad de expresión-censura" resulta funcional a los intereses de las grandes empresas que operan en la red.(44)

El modelo de Brasil

En abril/2014, el Congreso de Brasil aprobó por ley el "Marco Civil de Internet"(45), una especie de Constitución Nacional de Internet en ese país que establece los derechos, deberes y garantías de los usuarios y de las empresas proveedoras de servicios y aplicaciones, tanto locales como extranjeras. Los principios básicos de funcionamiento son la libertad de expresión y el derecho a la privacidad de las comunicaciones, tanto así como la importancia a la neutralidad de las comunicaciones en la red(46) y la libertad de empresa.

(42) Organización de las Naciones Unidas (ONU): "Declaración de Principios de Ginebra de la Cumbre Mundial de la Información" - Publicación de las Naciones Unidas - Ginebra - 2003 - pág. 5

(43) Gore, Albert: "Discurso de apertura de la Conferencia sobre el Desarrollo Global de las Telecomunicaciones de la Unión Internacional de Telecomunicaciones (UIT)" - Bs. As. - 21/3/1994

(44) Sain, Gustavo: "De consumidores a ciudadanos en línea" - Diario Página 12 - 12/5/2014

(45) L. 12965 de 2014 de la República Federativa de Brasil

(46) Este principio incluye una serie de nociones relacionadas con la imposibilidad, por parte de los proveedores de acceso a internet y de servicios de contenido, de obstaculizar o alterar en forma arbitraria las comunicaciones y la transferencia de datos. En este punto, los gobiernos deben actuar para el mantenimiento de la neutralidad de las comunicaciones a través de su intervención, regulando el servicio mediante el establecimiento de protocolos, la instrumentación de medidas administrativas o legislación que establezca reglas claras para las empresas

Uno de los puntos destacados de la norma es que estipula que las empresas proveedoras de servicio extranjeras deben adecuar los términos y condiciones de uso de sus servicios a la legislación local en materia de privacidad. Esto aplica cuando se colectan datos de usuarios en el territorio brasileño o cuando en las comunicaciones interviene al menos un dispositivo alojado en el país. En relación a esto, el Marco Civil prevé una serie de sanciones administrativas a las empresas que incumplan con estos principios entre las que se incluyen la suspensión del servicio y prohibición de actividades, sin perjuicio de otras sanciones de tipo administrativas o penales.

La norma estipula además que las empresas deben guardar sus registros de conexión de sus clientes tales como nombre real, datos filiatorios, nombres de usuario, día y hora de conexión, etc.; y los registros de acceso a aplicaciones, que incluyen contenidos de comunicaciones privadas a la que solo se pueden acceder únicamente mediante autorización judicial. En cuanto a las responsabilidades legales de los ISP, la ley estipula que las empresas no tienen responsabilidad civil por los contenidos publicados por terceros, salvo que los administradores sean conscientes de la existencia de dicho material dentro de sus plataformas y no los remueva. Bajo estos casos, las empresas deben comunicar al usuario que está violando la ley para que los elimine.

Un ejemplo de aplicación del Marco Civil se dio en diciembre/2015, donde una jueza de primera instancia de San Pablo ordenó a las empresas de telefonía celular bloquear el uso de WhatsApp durante 48 horas por el delito de obstrucción a la justicia, fundamentalmente por la negativa de la empresa Facebook -dueña de la aplicación- a responder las solicitudes de información en el marco de una investigación criminal por narcotráfico. Según el juzgado, la empresa se negó a facilitar datos de las comunicaciones de un presunto traficante del Primer Comando de la Capital (PCC) en dos oportunidades, lo que le valió de multas previas al fallo.(47)

En cuanto al órgano de aplicación de la ley, en Brasil existe un Comité Gestor de Internet (CGI), organismo central de internet con competencia en todo el territorio nacional. La historia del CGI se inicia en mayo/1995 cuando el Ministerio de Comunicaciones y el Ministerio de Ciencia, Tecnología e Innovación suscriben una nota acerca de la importancia de contar con un organismo para tal objetivo. A fin de ese mes, mediante una resolución interministerial, se crea el organismo, por aquel entonces con una misión puramente técnica, básicamente en la regulación de la prestación de servicio en relación a la interconexión y distribución de redes. En cuanto al diseño de políticas, por aquel entonces el CGI tenía un rol orientador, brindando recomendaciones y opinando sobre determinados temas, sin resolver en forma ejecutiva. Entre los objetivos explicitados en la resolución figuraban la libre y justa competitividad entre proveedores de servicio y el establecimiento de patrones de conducta entre usuarios y proveedores.

En el año 2003 se crea el Grupo de Trabajo de Seguridad en Redes (GTS) y durante ese mismo año, a su vez, el CGI se institucionaliza formalmente mediante decreto, donde también se establece el modelo de gobierno de internet en Brasil ampliando sus competencias iniciales. De acuerdo con la norma, sus atribuciones son:

- Establecer directrices estratégicas para el funcionamiento de la red en Brasil, las relaciones entre el gobierno y la sociedad y los números y nombres de dominio.
- Proponer programas de investigación para el desarrollo de internet en el territorio respecto a la calidad técnica de uso.

(47) "Por qué Brasil se quedó sin WhatsApp por orden judicial" - Sitio web de la BBC Mundo - 2/5/2016

- Recomendar normas, procedimientos y patrones técnicos operativos para la seguridad de las redes y servicios de internet.
- Articular normas y procedimientos para la regulación de actividades en la red.

A diferencia de la resolución de creación del CGI, a partir de 2003 se estipuló que el organismo tiene como misión principal la de establecer las normas básicas de funcionamiento de la red dentro de Brasil, realizar investigación y desarrollo en el área y regular actividades, más allá de las habituales funciones técnicas[48]. Finalmente en 2009, el organismo aprueba los 10 *Principios para la gobernanza de internet*, entre los que se destacan:

- El uso de internet basado en la libertad de expresión, la privacidad del individuo y el respecto a los derechos humanos.
- El establecimiento de un gobierno de internet participativo y democrático, con la intervención de varios sectores.
- El acceso universal a la red como factor de desarrollo humano y social.
- Respeto a la diversidad cultural.
- Promover la innovación tecnológica.
- La aplicación del principio de neutralidad de la red, donde se establece que el filtrado y privilegio de tráfico se deben centrar en criterios técnicos y éticos.
- Los principios de funcionalidad, seguridad y estabilidad, que alude al cumplimiento de normas técnicas de calidad respecto a estándares internacionales.
- Interoperabilidad.[49]

La necesidad de políticas públicas en materia de ciberseguridad

Desde la Revolución francesa en adelante y el surgimiento de la República como forma de organización política, *los Estados tienen la facultad indelegable de garantizar los derechos y libertades de los ciudadanos dentro de un determinado territorio* en cuanto

(48) En cuanto a la composición actual, el comité posee 21 miembros. La mayoría de ellos lo posee el sector gubernamental, con 9 representantes, seguido por el tercer sector y el sector empresarial con 4 cada uno, luego hay 3 plazas ocupadas por especialistas de la comunidad científica y económica y un notable sobre los asuntos de internet. Bajo la coordinación del Ministerio de Ciencia y Tecnología se incorporan organismos tales como:

- Casa Civil de Presidencia de la República.
- Ministerio de Defensa.
- Ministerio de Desarrollo, Industria y Comercio Exterior.
- Ministerio de Planeamiento, Presupuesto y Gestión.
- Agencia Nacional de Telecomunicaciones.
- Consejo Nacional de Desarrollo Científico y Tecnológico.
- Foro Nacional de Secretarios Estaduales para Asuntos de Ciencia y Tecnología.

Además se incluye:

- Un (1) profesional destacado en el área de internet.
- Cuatro (4) representantes del sector empresarial.
- Cuatro (4) de la sociedad civil.
- Tres (3) de la comunidad científica y tecnológica.

Entre los representantes del sector empresarial se encuentran los proveedores de contenido de internet, de la industria de telecomunicaciones informática y *software*, y los proveedores de infraestructuras

(49) Documentación extraída del sitio web del Comité Gestor de Internet de Brasil

a su integridad y libertad, tanto así como el de proteger sus bienes; es un principio fundacional de estos que no puede dejarse en manos del sector privado. Desde la apertura comercial de internet, los delitos informáticos adquirieron una nueva dimensión dentro de la agenda gubernamental de los países. A partir de la digitalización de la información de las personas y su almacenamiento en bases de datos, la realización de operaciones financieras en línea y el establecimiento de comunicaciones privadas en entornos virtuales, el principal temor que poseen los Estados frente a los principios liberales que promulgan los gigantes de internet y el gobierno de los Estados Unidos en nombre de la libertad de expresión es ser tildados de "censores" ante cualquier intento de regulación. En la actualidad, el cumplimiento de los principios básicos de Internet tales como la libertad de expresión, el derecho a la intimidad y el derecho a la información se encuentran en manos de las empresas proveedoras.

En este marco, la mayoría de las resoluciones técnicas y administrativas que obtienen los delitos informáticos que se cometen en la red son llevadas a cabo por bancos, empresas y organizaciones que operan en la web. Como se señaló anteriormente, cuando existe una conducta lesiva que afecta un derecho individual debe ser el Estado quien se encargue de restituir el mismo a través de la justicia, tanto así como para velar en el mantenimiento de dichos derechos para tratar de evitar de manera preventiva la comisión de hechos ilícitos que se produzcan en cualquier entorno, sea físico y virtual. Dicha función no puede ser *delegada al sector privado, ya que su fin principal es el lucro y no el interés general, motivo por el cual los usuarios son potenciales consumidores en una economía de mercado desregulada.* Esto resulta independiente de la responsabilidad social empresaria y de la existencia de políticas de contenidos apropiadas en los sitios que puedan establecer reglas de juego claras y sanciones equitativas a las personas que participan de los mismos dentro de sus facultades. La intervención de los gobiernos en materia de prevención de seguridad es un tema poco abordado en los diferentes foros de gobernanza de internet en el seno de los organismos internacionales que tratan estas problemáticas o las asociaciones que administran la red como la ICANN. Cabe señalar que el diseño de políticas públicas en materia de cibercrimen nada tiene que ver en la intervención en las comunicaciones privadas de los usuarios, e inclusive de la propiedad privada de dichas empresas proveedoras de servicio de internet. Las intervenciones deben darse en un marco de estricta legalidad establecida con una ley principal de internet que regule el funcionamiento de la red en un determinado país como manifestación soberana de un Estado.

Pero ¿a qué nos referimos cuando hablamos de políticas públicas en materia de ciberseguridad? Quizá se pueda entender el alcance de la importancia de las mismas con un ejemplo. En la Ciudad Autónoma de Buenos Aires, la Legislatura Porteña prohibió por ley el desarrollo de juegos de azar en esa jurisdicción en 2001[50]. La aprobación de dicha norma llevó al Poder Ejecutivo a instrumentar una serie de medidas orientadas a la prohibición de casinos o salas de juegos en el mundo físico. Si el espíritu de la ley que motivó a los legisladores fue el de evitar la ludopatía entre la población, en la actualidad cualquier ciudadano que habita en esa jurisdicción puede jugar y apostar desde la comodidad de su hogar a través de un juego de azar en línea, sitios de apuestas o en un casino por internet. Desde este punto de vista, los objetivos de la ley fracasan en tanto que su aplicación es parcial. En este sentido, no existe discusión en relación a que el Estado debe tener una política al respecto en relación a ello. En este caso se puede discutir los

(50) L. 455 de la CABA

alcances de la medida en el marco de la legalidad pero no las facultades de la autoridad administrativa de hacer cumplir la ley. Un ejemplo de políticas en este sentido podrían ser ordenar a las empresas de tarjetas de crédito prohibir su uso en estos sitios en la Ciudad Autónoma de Buenos Aires, asimismo, podría ordenarse a los proveedores de acceso al servicio de Internet a bloquear dichas páginas web, tanto así como la imposibilidad de descargas de aplicaciones de juegos de azar en teléfonos inteligentes en el área en cuestión a partir de la identificación de las direcciones IP de los dispositivos o bloquearlos.

Otro ejemplo claro lo representa la protección de los derechos de los sectores vulnerables en la red, como lo son los niños, niñas y adolescentes en el uso de servicios y aplicaciones de internet. En el mundo físico existen diferentes salones de juegos o recreación orientados a menores de edad, donde los padres pueden dejar a sus hijos por determinado período de tiempo tras la realización de un evento (cumpleaños, comuniones, aniversarios etc.). En los mismos y bajo la supervisión de personal autorizado, se desarrollan actividades lúdicas relacionadas con espacios de juegos (peloteros, laberintos, hamacas, saltarines), actividades artísticas o musicales y espectáculos varios brindados por los animadores del lugar. En tanto espacio privado orientado a menores de edad, su habilitación está sujeta a una serie de normas y reglas de seguridad establecidas por el ente de control y habilitación jurisdiccional. Algunos de ellos son: servicios de emergencias médicas y seguro de responsabilidad civil contratados, botiquín y servicios de primeros auxilios y matafuegos, cumplimientos de normas de calidad preestablecidas que hacen a la habilitación de los juegos y de las instalaciones eléctricas, realización de inspecciones periódicas para verificar el estado y el mantenimiento de los juegos mecanismos o de impacto y la habilitación de personal idóneo para el cuidado de niños y niñas, entre otras medidas. Más allá de las diferencias obvias entre lo físico y lo digital ¿por qué los entornos virtuales de la red orientados a niños, niñas y adolescentes -juegos de rol en línea, chats para menores, el perfil o un canal de una red social o un canal de YouTube- no deben ser sometidos diferentes medidas de control y supervisión por las autoridades correspondientes? En la actualidad, tanto el diseño de un entorno virtual como las reglas de uso de un servicio o aplicación en la web es establecida únicamente por la empresa que lo administra.

En la República Argentina la mayoría de las denuncias judiciales que reciben están relacionadas con delitos contra la integridad sexual de menores de edad por parte de pedófilos. En este sentido, ¿desde qué punto de vista exigir entornos virtuales óptimos para los menores en juegos en línea, por ejemplo, o la presencia de moderadores en charlas y personas que supervisen contenidos ilícitos como material pornográfico resulta un atentado a la libertad de expresión? ¿Cuál sería el motivo por el cual los espacios físicos deben estar sometidos a normas de habilitación y control y no así los espacios virtuales en la nube? Más allá de la tipificación de conductas ilícitas relacionadas con dispositivos informáticos y el fortalecimiento de la cooperación internacional en materia judicial y la existencia de organismos técnicos abocados a la seguridad informática, *cada país debe tener una política pública en materia de ciberseguridad, una ley que regule el funcionamiento de internet en un determinado país y un organismo rector de aplicación abocado al desarrollo y regulación de la red dentro de su territorio.*

En cuanto a una *ley marco para el funcionamiento de internet*, al igual que el marco civil brasileño debe oficiar a modo de constitución nacional dentro de un determinado país, estableciendo derechos, deberes y garantías de los usuarios y las obligaciones que deben someterse las empresas proveedoras de acceso, servicios y aplicaciones y otras que operen en la red dentro de ese territorio. Más allá de los alcances de la ley

brasileña, la misma no solo debe establecer principios jurídicos en el plano civil, sino también administrativo, comercial y penal. En líneas generales, una ley marco de estas características debería contemplar, entre otras cosas:

- Los alcances de la norma y las facultades del órgano de aplicación por sobre las empresas que operan en internet dentro del territorio, sean nacionales o extrajeras independiente a partir de la utilización de un usuario cualquiera fuese su nacionalidad dentro del territorio brasileño.
- El reconocimiento tácito de una "sucursal" de las empresas extranjeras que operan en la red en tanto estén disponibles para su acceso o uso dentro del territorio en cuestión sin la necesidad que se encuentren sus servidores dentro del país ni posea una sede legal en el mismo.
- La obligatoriedad para las empresas extranjeras a adaptar sus términos y condiciones de uso de sus servicios y aplicaciones a la normativa local, no solo en términos de privacidad de los datos sino también en materia de seguridad de las personas. Las empresas deben advertir de las consecuencias legales de determinados comportamientos dentro de las políticas de uso y contenidos de un sitio o el uso de un determinado programa.
- Responsabilidades y obligaciones administrativas, civiles, penales y comerciales de las empresas proveedoras que brinde Internet que operan dentro del territorio, tanto así como las sanciones correspondientes en caso de incumplimiento.
- La condición por parte de las empresas proveedoras de servicios y aplicaciones a notificar a las autoridades competentes conductas indebidas por parte de sus usuarios que constituyan un delito de acuerdo a la normativa local.
- La ilegalidad por parte de empresas proveedoras de hacer uso de los datos personales de sus usuarios para fines comerciales son el consentimiento expreso de los mismos, tanto así como el reporte periódico para que fueron utilizados los mismos a aquellos que acepten dicha condición.
- La imposibilidad de cualquier organismo de gobierno a solicitar datos personales de determinados usuarios o contenidos de comunicaciones privadas salvo en caso expreso por parte de un tribunal competente en el marco de una investigación criminal.
- La obligatoriedad por parte de las empresas de conservar los registros de conexión y de acceso por un período determinado para ponerlas a disposición de la justicia en el marco de una causa en curso.
- La creación de un órgano de aplicación de la ley que oficie de organismo central de regulación de internet dentro del territorio.

En relación con el último punto, dicho organismo, además de velar por la aplicación de la ley marco, debe ser el responsable de aplicar las sanciones que contempla la norma en términos administrativos y realizar las denuncias a los tribunales correspondientes en los planos civil, comercial y penal en caso de incumplimiento. Asimismo estará facultado para ejecutar las directrices básicas mediante resoluciones vinculantes de tipo administrativa en lo que hace al funcionamiento de internet en el país. Entre sus funciones se destacan:

- Instrumentación de políticas, estrategias y líneas de acción generales y particulares desde un punto de vista técnico y de desarrollo.
- La realización de estudios criminológicos e informes estadísticos sobre el desarrollo de internet en el país y en materia de cibercrimen.

- Asesoramiento a organismos competentes de la administración pública a nivel nacional, provincial o municipal respecto al cumplimiento de sus misiones, funciones y competencias en la red.
- Asistencia legal a víctimas de delitos informáticos y orientación acerca de denuncias sobre las mismas.
- Centralizar las funciones de registración de direcciones web en relación con el dominio del país, las funciones establecidas por los organismos gubernamentales que oficien como CERT en un determinado país, establecer un registro de proveedores nacionales y extranjeros que brindan diferentes servicios en la red y el órgano abocado a la protección de datos personales.

En materia de cibercrimen, es el organismo encargado de *llevar adelante la política de prevención de seguridad en internet en determinado país*, motivo por el cual tendrá facultades para:

- Establecer canales de denuncia directa en sitios web mayormente visitados con organismos competentes o fiscalías especializadas.
- Dictaminar política de seguridad para entornos virtuales gráficos y verificar su efectivo cumplimiento por parte de empresas proveedoras que operan en internet.
- Establecimiento de habilitación de bases de datos personales en el país bajo mecanismos de supervisión de medidas de seguridad óptimas para el almacenamiento y la transmisión.
- Verificación de adaptación de los términos y condiciones de usos de los servicios en materia de seguridad.
- Generar acuerdos de cooperación entre organismos de gobierno y empresas proveedoras para la realización de campañas de concientización sobre un uso seguro y responsable de entornos virtuales.

VI - CONCLUSIÓN

Si bien resulta necesaria la tipificación de conductas indebidas, hechos ilícitos e ilegales por parte del derecho penal, civil o comercial; la cooperación internacional en este sentido y la reforma de los códigos procesales para la admisibilidad de pruebas electrónicas en el marco de una causa judicial, la solución penal resulta insuficiente en términos de diseño de una política pública para la red. En este sentido, resulta necesaria la creación en el seno de las administraciones centrales de un organismo gubernamental para el diseño de estrategias y políticas integrales en materia de cibercrimen. Las políticas resultantes deben estar fundadas en diagnósticos certeros basados en la realización de estudios y el acopio de información estadística sobre nuevas modalidades delictivas. A su vez, debe proponer legislación para la regulación del sector y brindar asistencia y asesoramiento a aquellos organismos que así lo requieran, brindando recomendaciones y líneas de acción estratégicas.

Algunas cuestiones sobre delitos informáticos en el ámbito financiero y económico. Implicancias y consecuencias en materia penal y responsabilidad civil

Matilde S. Martínez(*)

I - INTRODUCCIÓN

Con el advenimiento del fenómeno informático se ha originado una revolución en todo el mundo, lo que nos permite afirmar que estamos siendo protagonistas de una nueva era: la era "informática". Así, se ha sostenido que "*en la sociedad del siglo XXI se ha producido el tránsito de la era industrial a la de la información, nuestra economía se ha convertido en una economía de la información. La era industrial se basó en la producción, mientras que la era de la información se fundamenta en la comunicación y la información electrónica, ambas a gran escala*".(1)

Las Tecnologías de la Información y Comunicación (TIC), seguidas de una vertiginosa evolución, han generado una nueva forma de poder, "el poder informático". Este nuevo poder no ha sido indiferente al derecho, que debe adoptar, por un lado, la postura de legitimarlo en virtud de los magníficos beneficios que proporciona a los individuos; por otro lado, debe adoptar una postura contenedora, debido a los peligros que puede ocasionar a las personas. Se van creando nuevas herramientas jurídicas tendientes a la protección frente a los abusos de este nuevo poder(2). Ante ello, se ha considerado que existe un derecho informático como rama autónoma del derecho con

(*) Abogada. Especialista universitaria de Protección de Datos Personales y Privacidad (Facultad de Derecho, Universidad de Murcia). Profesora de la Carrera de Especialización en Derecho Informático (UBA)

(1) Altmark, Daniel R. y Molina Quiroga, Eduardo: "Tratado de derecho informático" - LL - Bs. As. - 2012 - T. I - pág. 1

(2) Martínez, Matilde S.: "Hábeas data financiero" - Ediciones de la República - Bs. As. - 2009 - pág. 101

legislación, doctrina, jurisprudencia, formación académica y universitaria con principios propios. Fernández Delpech explica que "*podríamos definir al derecho informático como el conjunto de principios y normas que regulan los efectos jurídicos nacidos de la interrelación entre el derecho y la informática. Y que la informática es una ciencia que estudia métodos, proceso y técnicas, con el fin de almacenar, procesar y transmitir informaciones y datos en formato digital*".(3)

Al hablar de tecnología informática debemos incluir incuestionablemente a Internet, que ha modificado ostensiblemente los medios de información y comunicación en la sociedad global.

Además, la aplicación de la informática es ilimitada: no solo abarca la ciencia de la computación, el *software* y el *hardware*, sino que también proporciona beneficios en el desarrollo de negocios, almacenamiento y proceso de información, en medicina, transportes, inteligencia artificial, entre otras tantas áreas.

El Dr. Altmark sostiene que "*la informática es la disciplina que estudia el fenómeno de la información, y la elaboración, transmisión y utilización de la información principalmente, con la ayuda de ordenadores y sistemas de telecomunicación como instrumentos*". Y agrega que la "*informática es la aplicación racional y sistemática de la información para el desarrollo económico, social y político*".(4)

Así como las nuevas tecnologías han contribuido a este desarrollo "económico, social y político", influyendo en el avance de las potencialidades de los individuos, también se han multiplicado las posibilidades de cometer conductas disvaliosas, dañinas y peligrosas contra terceras personas, las cuales denominamos en general "delitos informáticos" y que en muchos casos trascienden las fronteras, alcanzando una efectiva progresión global. Suelen utilizarse indistintamente los términos "delincuencia informática", "delincuencia de alta tecnología", "delincuencia cibernética", "ciberdelincuencia", "delincuencia relacionada con los ordenadores" o "actividades delictivas realizadas con la ayuda de redes de comunicaciones y sistemas de información electrónica"(5). Además, Altmark expresa que "*se trata de conductas antijurídicas no tan ordinarias, pues suponen un mínimo de conocimientos y de acceso a la tecnología, que se realizan a partir de un sistema, utilizando a éste como un instrumento eficaz para lograr el objetivo delictivo perseguido, ya sea manipulando el soporte lógico de aquél, o bien utilizando ilegítimamente los datos y programas de un sistema, o bien utilizando correctamente el sistema pero para introducirse en otro u otros y producir un resultado disvalioso en bienes económicos o personales de otros sujetos*".(6)

En cuanto al concepto de delito informático, podríamos citar lo manifestado por Marcos Salt, que considera que "*abarca un conjunto de conductas de distintas características que afectan bienes jurídicos diversos y que son agrupadas bajo este concepto por su relación con el ordenador*".(7)

(3) Fernández Delpech, Horacio: "Manual de derecho informático" - Ed. AbeledoPerrot - Bs. As. - 2014 - pág. 1

(4) Altmark, Daniel R. y Molina Quiroga, Eduardo: "Tratado de derecho informático" - LL - Bs. As. - 2012 - T. I - pág. 2

(5) Altmark, Daniel R. y Molina Quiroga, Eduardo: "Tratado de derecho informático" - LL - Bs. As. - 2012 - T. III - pág. 285

(6) Altmark, Daniel R. y Molina Quiroga, Eduardo: "Tratado de derecho informático" - LL - Bs. As. - 2012 - T. III - pág. 226

(7) Salt, Marcos: "Informática y delito" - Revista Jurídica C.E. - Bs. As. - 1997 - págs. 6/21

En términos generales, podríamos clasificar estas conductas antijurídicas o delitos informáticos de acuerdo al bien jurídico protegido en los siguientes grupos:

a) los que se cometen a través de las redes sociales como atentados a la intimidad, el honor y la integridad moral[8] en sus distintas formas;
b) delito de *stalking* como una conducta intencionada y maliciosa de persecución, acecho o acoso contra una persona[9] que puede llevarse a cabo a través de Internet o de otros medios;
c) delitos sexuales contra los menores (*online grooming*), ataques a través de medios tecnológicos o el uso de drogas[10];
d) ciberpornografía infantil con la utilización de sitios web donde se realiza tráfico de material pornográfico de menores de edad[11];
e) "ciberodio", que comprende la xenofobia, el racismo, el odio y la discriminación[12];
f) delitos contra la propiedad intelectual; y
g) estafas y fraudes como aquellas conductas que atentan contra el patrimonio de terceras personas.

Para que estas conductas disvaliosas sean consideradas delitos deben encuadrarse en el tipo penal correspondiente. Ello debido al respeto por el principio de legalidad que establece que no puede haber delito ni pena sin una ley previa a la comisión del hecho, según lo establece el principio *nulla poena sine lege*.

En el presente trabajo nos ocuparemos de analizar las conductas sobre estafas y fraudes, es decir, aquellas donde el bien jurídico protegido es el *patrimonio* de las personas.

II - LOS DELITOS INFORMÁTICOS EN ARGENTINA

En un principio, el Código Penal (CP) de la República Argentina no tenía normas jurídicas que tipificaran los delitos que se originaban como consecuencia del uso de las nuevas tecnologías de la comunicación y la información. Paulatinamente comenzaron a aparecer figuras penales relacionadas con esta temática en diferentes leyes especiales. Siguiendo a Fernández Delpech, podemos mencionar: "*Los delitos relacionados con los derechos de autor contemplados en la* ley 11723 *de Propiedad Intelectual; Los delitos creados por la* ley 25326 *de Protección de Datos Personales; La sustracción de secretos comerciales contenidos en soportes informáticos, figura contemplada en la ley 24766 de Confidencialidad; La alteración dolosa de registros, establecida como delito en los arts. 12 y 12 bis, ley Penal Tributaria 24769; Delitos tipificados en la ley 23592 Antidiscriminatoria*"[13]. La ley 26904, publicada en el Boletín Oficial el 11/12/2013, incorpora al CP el delito de *grooming* en el artículo 131, que establece que "*será penado con prisión de seis meses a cuatro años el que, por medio de internet, del teléfono o de 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*".

(8) Riquert, Marcelo A. (Coord.): "Ciberdelitos" - Ed. Hammurabi - Bs. As. - 2014 - pág. 215
(9) Riquert, Marcelo A. (Coord.): "Ciberdelitos" - Ed. Hammurabi - Bs. As. - 2014 - pág. 233
(10) Riquert, Marcelo A. (Coord.): "Ciberdelitos" - Ed. Hammurabi - Bs. As. - 2014 - pág. 254
(11) Riquert, Marcelo A. (Coord.): "Ciberdelitos" - Ed. Hammurabi - Bs. As. - 2014 - pág. 278
(12) Riquert, Marcelo A. (Coord.): "Ciberdelitos" - Ed. Hammurabi - Bs. As. - 2014 - pág. 312
(13) Fernández Delpech, Horacio: "Manual de derecho informático" - Ed. AbeledoPerrot - Bs. As. - 2014 - págs. 198 y 213

Cada vez se hace más necesario continuar trabajando en materia legislativa sobre los delitos cibernéticos; así, existen varios proyectos de leyes que tratan nuevas figuras disvaliosas que no se encuentran tipificadas como delitos y por lo tanto no tienen asignado un castigo legal.

Una prestigiosa doctrina entiende "*que una clasificación de las distintas modalidades delictivas relacionadas con la informática debe hacerse con relación al bien jurídico protegido, y dentro de esta categoría, distinguir las acciones típicas que la vida cotidiana o la experiencia local o comparada nos dan noticia. De esta forma se centrarán las bases para fijar una adecuada política de reforma del Código Penal en materia de delitos informáticos que contemple las verdaderas necesidades que requiere nuestra legislación criminal*".(14)

A propósito de lo anterior, en el año 2008 se sancionó la ley 26388(15), que se la conoce como la ley de delitos informáticos. Esta norma tipifica como delitos e incorpora al CP varias conductas relacionadas con el uso de las nuevas tecnologías.

Las nuevas conductas tipificadas como figuras penales las presentamos de acuerdo a la clasificación realizada por la prestigiosa doctrina(16):

a) Daño informático, agregándose en el artículo 183 del CP como segundo párrafo: "*En la misma pena incurrirá el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daño*".

b) Fraude informático, incorporando el inciso 16) al artículo 173 del CP en los siguientes términos: "*El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos*".

c) Alteración de pruebas, sustituyendo el artículo 255 del CP por el siguiente texto: "*Será reprimido con prisión de un mes a cuatro años, el que sustrajere, alterare, ocultare, destruyere o inutilizare en todo o en parte objetos destinados a servir de prueba ante la autoridad competente, registros o documentos confiados a la custodia de un funcionario público o de otra persona en el interés del servicio público. Si el autor fuera el mismo depositario, sufrirá además inhabilitación especial por doble tiempo. Si el hecho se cometiera por imprudencia o negligencia del depositario, este será reprimido con multa de pesos setecientos cincuenta a pesos doce mil quinientos*".

d) Pornografía infantil, sustituyendo el artículo 128 del CP por el siguiente: "*Será reprimido con prisión de tres a seis años al que produjere, financiare, ofreciere, comerciare, facilitare, divulgare o distribuyere, por cualquier medio, toda representación de un menor de dieciocho 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*

(14) Altmark, Daniel R. y Molina Quiroga, Eduardo: "Tratado de derecho informático" - LL - Bs. As. - 2012 - T. I - pág. 239

(15) Sancionada 4/6/2008. Promulgada de hecho 24/6/2008. Infoleg (consultado 7/5/2018)

(16) Fernández Delpech, Horacio: "Manual de derecho informático" - Ed. AbeledoPerrot - Bs. As. - 2014 - págs. 197/213

distribución o 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 catorce años. Todas las escalas penales previstas en este artículo se elevarán en un tercio en su mínimo y en su máximo cuando la víctima fuere menor de trece años". Este artículo fue modificado por la ley 27436[17] del 21/3/2018, fundamentalmente para penalizar la simple tenencia de pornografía infantil y el agravamiento de las penas impuestas de cada una de las figuras descriptas.

e) Delitos contra la privacidad: en primer lugar, la ley 26388 modifica el epígrafe del Capítulo III, del Título V, del Libro II del CP por el siguiente: "Violación de Secretos y de la Privacidad". Luego sustituye el artículo 153 del mismo texto legal por: "*Será reprimido con prisión de quince días a seis meses el que abriere o accediere indebidamente a una comunicación electrónica, una carta, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, que no le esté dirigido; o se apoderare indebidamente de una comunicación electrónica, una carta, un pliego, un despacho u otro papel privado, aunque no esté cerrado; o indebidamente suprimiere o desviare de su destino una correspondencia o una comunicación electrónica que no le esté dirigida. En la misma pena incurrirá el que indebidamente interceptare comunicaciones electrónicas o telecomunicaciones provenientes de cualquier sistema de carácter privado o de acceso restringido. La pena será de prisión de un mes a un año, si el autor además comunicare a otro o publicare el contenido de la carta, escrito, despacho o comunicación electrónica. Si el hecho lo cometiere un funcionario público que abusare de sus funciones, sufrirá además, inhabilitación especial por el doble del tiempo de la condena*". Además se incorpora al CP el artículo 153 bis en los siguientes términos: "*Será reprimido con prisión de quince días a seis meses, si no resultare un delito más severamente penado, el que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido. La pena será de un mes a un año de prisión cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros*". Adicionalmente se sustituye el artículo 155 del CP por el siguiente: "*Será reprimido con multa de pesos un mil quinientos a pesos cien mil, el que hallándose en posesión de una correspondencia, una comunicación electrónica, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, no destinados a la publicidad, los hiciere publicar indebidamente, si el hecho causare o pudiera causar perjuicios a terceros. Está exento de responsabilidad penal el que hubiere obrado con el propósito inequívoco de proteger un interés público*". También se sustituye el artículo 157 del CP expresando: "*Será reprimido con la pena de prisión de un mes a dos años e inhabilitación especial de uno a cuatro años, el funcionario público que revelare hechos, actuaciones, documentos o datos, que por ley deben ser secretos*". Otra sustitución es la del artículo 157 bis que queda redactado de la siguiente manera: "*Será reprimido con pena de prisión de un mes a dos años el que: 1. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales; 2. Ilegítimamente proporcionare o revelare a otro información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley. 3. Ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales. Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de un a cuatro años*".

(17) BO: 23/4/2018

f) Delitos contra la seguridad pública e interrupción de las comunicaciones: en relación con este delito se sustituye el artículo 197 del CP por el siguiente texto: "*Será reprimido con prisión de seis meses a dos años, el que interrumpiere o entorpeciere la comunicación telegráfica, telefónica o de otra naturaleza o resistiere violentamente el restablecimiento de la comunicación interrumpida*".

g) Falsificación de documentos electrónicos: en este caso se incorporan como últimos párrafos del artículo 77 del CP los siguientes: "*El término 'documento' comprende toda representación de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión. Los términos 'firma' y 'suscripción' comprenden la firma digital, la creación de una firma digital o firmar digitalmente. Los términos 'instrumento privado' y 'certificado' comprenden el documento digital firmado digitalmente*".

III - EL DELITO DE ESTAFA O FRAUDE INFORMÁTICO

En este apartado nos proponemos tratar el delito de estafa o fraude informático que atenta contra el patrimonio de terceras personas, que "*al igual que en todas las causas de estafa, requiere para su configuración el causar un perjuicio de contenido patrimonial a otra persona*"[18]. El bien jurídico protegido es el patrimonio en general, y lo que se castiga son las conductas que afectan el patrimonio mediante el uso de sistemas informáticos por parte del causante.[19]

En nuestro ordenamiento jurídico penal, la figura típica y genérica de la estafa es el artículo 172 del CP que establece: "*Será reprimido con prisión de un mes a seis años, el que defraudare a otro con nombre supuesto, calidad simulada, falsos títulos, influencia mentida, abuso de confianza o aparentando bienes, crédito, comisión, empresa o negociación o valiéndose de cualquier otro ardid o engaño*".

Esta figura genérica de fraude no encuadraba completamente en el fraude informático, pues requiere "ardid en el autor del delito", "error en la víctima" y "perjuicio patrimonial" según Choclán Montalvo, citado por Alonso-Zapata. Explica la distinción entre "delito informático propiamente dicho" -que se reduce a la manipulación o afectación del *software* o parte lógica del sistema, donde se incluyen los datos almacenados- y el "delito informático en sentido lato" -que abarca el uso medial del sistema informático para perpetrar ataques al patrimonio-. Los autores citados consideran que "*la secuencia lógica reclamada por el delito de estafa (ardid-engaño-disposición patrimonial perjudicial) fracasa, a poco que se repare en los desafíos planteados por las nuevas tecnologías a la regulación penal. El clásico delito de estafa, tal como está regulado por el art. 172 del CP autóctono, no logra abarcar los casos donde no existe ninguna persona que actúa erróneamente a partir del ardid desplegado por el autor. En la actualidad, los sistemas bancarios están completamente informatizados y la distribución del dinero se encuentra automatizada*"[20]. El artículo 172 del CP tipifica una serie de conductas fraudulentas, las que son reprimidas con prisión de un mes a seis años.

(18) Juz. Fed. San Isidro N° 1 Sec. N° 2, Sec. Penal N° 1 - Sala I "Inc. de apelación del procesamiento de B" - San Martín - 7/6/2013

(19) Aboso, Gustavo E. y Zapata, María F.: "Cibercriminalidad y derecho penal" - IB d F. Montevideo-Bs. As., en Argentina Euros Editores SRL - 2006 - pág. 71

(20) Aboso, Gustavo E. y Zapata, María F.: "Cibercriminalidad y derecho penal" - IB d F. Montevideo-Bs. As., en Argentina Euros Editores SRL - 2006 - pág. 72

En los casos de fraude informático es necesario descartar el error de la víctima llevada a cabo por el ardid o engaño del autor, pues este manipula una máquina con el objeto de obtener un beneficio económico en perjuicio patrimonial del afectado.

En principio, el uso masivo de tarjetas de compra en el comercio produjo la necesidad de regular las conductas fraudulentas llevadas a cabo a través de este instrumento de pago. Mediante la ley 25930[21] se incorporó al artículo 173 del CP el inciso 15), que contempla una vasta cantidad de fraudes con las tarjetas mencionadas, estableciendo que: "*El que defraudare mediante el uso de una tarjeta de compra, crédito o débito, cuando la misma hubiere sido falsificada, adulterada, hurtada, robada, perdida u obtenida del legítimo emisor mediante ardid o engaño, o mediante el uso no autorizado de sus datos, aunque lo hiciere por medio de una operación automática*".

Posteriormente, con la sanción de la ley 26388 ya comentada, conocida como la ley de "delitos informáticos", se incorpora el inciso 16) al artículo 173 del CP, el cual establece lo siguiente: "*El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos*". Con ello, ahora puede prescindirse de esta secuencia "ardid-error-perjuicio económico" y se amplían las posibilidades de encuadramientos de los distintos fraudes y estafas informáticas, incorporando cualquier forma de manipulación de un sistema informático con el objetivo de obtener un indebido beneficio económico en perjuicio de la víctima.

En relación con ello podemos observar jurisprudencia que así lo expresa: "*la disposición patrimonial debe ser consecuencia de cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos que produce el hecho lesivo. En esta dirección, se entiende como manipulación a cualquier modificación del resultado de un proceso automatizado de datos, a través de la alteración de los existentes o la introducción de nuevos, en cualquiera de las fases del proceso*"[22]. En el mismo sentido se imputa a R.M.G.G. y a M.J.R. por haber llevado a cabo maniobras de fraude mediante técnicas de manipulación informática *phishing* -página paralela-, por la que obtuvieron los datos necesarios -código de transferencia y número de tarjeta de crédito- para poder operar en las cuentas bancarias de E.R.R. y, así, efectuaron dos transferencias de dinero desde las cuentas de E.R.R. a la cuenta bancaria de los imputados.[23]

IV - LOS DELITOS DE FRAUDES FINANCIEROS Y ECONÓMICOS MÁS COMUNES

Entre los delitos más comunes que sufren el sistema financiero y los titulares de cuentas bancarias podemos mencionar la alteración de registros informáticos con el propósito de ingresar a cuentas bancarias y desviar fondos a las cuentas de los delincuentes.[24]

(21) BO: 21/9/2004

(22) Juz. Fed. San Isidro N° 1 Sec. N° 2, Sec. Penal N° 1 - Sala I "Inc. de apelación del procesamiento de B" - San Martín - 7/6/2013

(23) "G. R. y otro s/procesamientos" - CCrim. y Correc. Fed. - Sala VI - 3/8/2010 - Cita digital IUSJU184903D

(24) Fernández Delpech, Horacio: "Manual de derecho informático" - Ed. AbeledoPerrot - Bs. As. - 2014 - pág. 203

a) Fraudes con tarjetas

Los fraudes con tarjetas abarcan a las de compra, crédito o débito cuando son falsificadas, adulteradas, hurtadas, robadas, perdidas u obtenidas ilegítimamente, tal como lo prescribe el inciso 15) del artículo 173 del CP. En tal sentido se ha dicho "*que comete el delito de estafa en grado de tentativa el que utiliza la identidad y la tarjeta de crédito de otra persona para generar una compra a través de la red telemática*" ("D. y G., P. J. s/procesamiento estafa" - CN Crim. y Corr. - Sala V - 30/6/2003, c. 21.774). Asimismo, "*cuando el autor obtiene, de manera ilícita, una tarjeta de crédito de un tercero, al que le fue previamente sustraída, y la utiliza fraudulentamente mediante diversas extracciones dinerarias no autorizadas*" (BGH 2 StR 461/05, sentencia del 13/1/2006). También dispone que "*otro tanto se dijo de la conducta desplegada por los autores del espionaje de datos bancarios (en especial, claves de acceso), las que fueron utilizadas para la reproducción de falsas tarjetas de pago y así lograr consumar el fraude informático*" (BGH 3 StR 425/04, sentencia del 10/5/2005).[25]

Con acierto se ha expresado que el uso no autorizado de la tarjeta de crédito presenta una estructura de estafa triangular. El supuesto titular de la tarjeta engaña al comerciante sobre su identidad y de esta manera logra provocar el error. Pero el perjuicio patrimonial lo sufre la propia entidad emisora de la tarjeta como parte integral del riesgo inherente que implica la utilización fraudulenta por parte de terceros.[26]

Otra maniobra fraudulenta muy común utilizada por estafadores con tarjetas bancarias es el uso de estas en cajeros automáticos, ya sea con tarjetas adulteradas o auténticas pero sin autorización del titular de la cuenta para obtener un beneficio económico.

b) "*Phishing*" y "*pharming*"

Los delitos informáticos frecuentes en el ámbito financiero son el *phishing* y el *pharming*. En el primer caso, los *phishers* o estafadores simulan pertenecer a entidades bancarias y solicitan a los cibernavegantes los datos de tarjetas de crédito o las claves bancarias, a través de un formulario o un correo electrónico con un enlace que conduzca a una falsa página web con una apariencia similar a la original[27]. Si logran engañar al receptor del mensaje obtienen la clave de acceso a sus cuentas y realizan transferencias o retiros de dineros de esas cuentas.

Fernández Delpech define el *pharming* como *"una nueva modalidad de fraude* online *que consiste en suplantar el sistema de resolución de nombres de dominio (DNS) para conducir al usuario a una página web bancaria falsa y apoderarse de sus claves. Cuando un usuario teclea una dirección en su navegador, esta debe ser convertida a una dirección IP numérica. Este proceso es lo que se llama resolución de nombres, y de ello se encargan los servidores DNS. El* pharming *implica acceder al sistema de un usuario y modificar ese sistema de resolución de nombres, de manera que cuando el usuario crea que está accediendo a su banco en Internet, realmente está accediendo a la IP de una página web*

(25) Aboso, Gustavo E. y Zapata, María F.: "Cibercriminalidad y derecho penal" - Ed. Euros Editores - 2006 - págs. 78/9

(26) Aboso, Gustavo E. y Zapata, María F.: "Cibercriminalidad y derecho penal" - Ed. Euros Editores - 2006 - págs. 79

(27) "Bieniauskas, Carlos c/Banco de la Ciudad de Buenos Aires s/ordinario" - CNCom. - Sala D - 1/7/2008 - Cita digital IUSJU058123C

falsa"[28]. Es una maniobra más sofisticada y peligrosa que el *phishing*, ya que se encauza mediante la manipulación de las direcciones DNS. En este caso, mediante un correo electrónico vacío sobre el que se *clickea* se instala un programa que engaña al navegador del usuario y lo deriva a direcciones falsas. Al ser engañado, el usuario ingresará sus datos confidenciales sin temor, en tanto desconoce que se los está enviando a un delincuente[29]. En el caso que se cita, "*en el escrito de demanda el actor reconoció haber revelado el número* PIN *(sigla que refiere al* personal identification number *o* password*; en su versión castellana al código de identificación de acceso o clave personal) al ser sorprendido por terceros quienes mediante argucias obtuvieron que develara ese número secreto. Es indudable que el conocimiento de ese dato facilita la maniobra delictiva que a partir de allí se produjo*".[30]

Con referencia a estos delitos informáticos ha explicado el perito de la causa "P. y otros s/defraudación" "*que por lo general, y acorde a su experiencia en el tópico, estas maniobras defraudatorias son realizadas por personas con vastos conocimientos técnicos informáticos que se encuentran en países extranjeros. A su vez, los verdaderos titulares de las I.P. son herramientas de los autores, quienes infectan los* softwares *de estas personas a través de virus troyanos y la controlan mediante aplicaciones de la más variada índole allí instaladas, que no suelen dar a conocer su origen, o si lo hacen remiten a servidores en el exterior. Estos virus a los que se hace referencia permiten el acceso a un sistema remoto en el que se pueden realizar distintas acciones sin contar con permiso alguno de su titular, quien en la mayoría de estos casos siquiera tiene conocimiento de la invasión de sus datos personales*".[31]

En la causa "C., P. A. s/recurso de casación" la Cámara Federal de Casación Penal resolvió condenar a P.A.C. por ser autor penalmente responsable del delito de defraudación mediante técnicas de manipulación informática, con fundamento, entre otras normas, por el inciso 16) del artículo 173 del CP antes citado. En la causa se tuvo por acreditado que P.A.C., mediante la manipulación indebida de datos informáticos, obtuvo el usuario y contraseña de M.C.B., titular de una cuenta en el Banco Francés, para luego efectuar una transferencia de capitales mediante el sistema *home banking Francés-net* por la suma de pesos $ 3.000 hacia la cuenta bancaria que D.O.A. poseía en la misma entidad bancaria, desde la cual el dinero fue retirado por el nombrado.[32]

c) Ofertas de trabajo falsas

Se trata del envío de ofertas de trabajo falsas con el propósito de usar a estas personas para blanquear y enviar dinero robado a otros países[33]. Estas maniobras delictivas también suelen efectuarse a través del *phishing*.

(28) Fernández Delpech, Horacio: "Manual de derecho informático" - Ed. AbeledoPerrot - Bs. As. - 2014 - pág. 204

(29) Monasterky, Daniel y Costamagna, Clara: "Phishing - Pharming: nuevas modalidades de estafas online". Ver en El Dial

(30) "Bieniauskas, Carlos c/Banco de la Ciudad de Buenos Aires s/ordinario" - CNCom. - Sala D - 1/7/2008 - Cita digital IUSJU058123C

(31) "P. y otros s/defraudación" - Cám. Nac. Crim. y Correc. - Sala V - 24/10/2013 - Cita digital IUSJU226163D

(32) "C., P. A. s/recurso de casación" - CFed. Casación Penal - Sala III - 16/6/2015 - Cita digital IUSJU001828E

(33) Fernández Delpech, Horacio: "Manual de derecho informático" - Ed. AbeledoPerrot - Bs. As. - 2014 - pág. 204

Como tal, mencionamos la causa "P. y otros s/defraudación", donde se ha afirmado que se debe "*remarcar el concepto de* phishing *pues, acorde a las explicaciones brindadas por los imputados y la documentación que han logrado aportar a efectos de sustentar sus dichos, surge con meridiana claridad que estos, al igual que los damnificados que sufrieron sustracciones dinerarias de sus cuentas bancarias, habrían sido engañados por los verdaderos autores de la maniobra, de momento desconocidos. De los dichos vertidos por todos ellos al momento de ser convocados a prestar declaración indagatoria surge un denominador común y varios puntos de coincidencia que marcan la pauta de que todos habían sido víctimas de una misma maniobra delictiva en la cual actuaron -engañados- como meros instrumentos que obraron sin dolo de los verdaderos autores del ilícito que, de ser detectados, serán considerados autores mediatos. Al respecto, ha explicado la doctrina que 'el rasgo fundamental de la autoría mediata reside en que el autor no realiza personalmente la acción ejecutiva, sino mediante otro (instrumento); y lo que caracteriza el dominio del hecho es la subordinación de la voluntad del instrumento a la del autor mediato', que en este caso en particular se verifica a través de la relación laboral simulada. En este mismo contexto, 'la primera hipótesis de la autoría mediata se da en el caso del que utiliza, como medio para alcanzar el fin propuesto, a otro cuya acción -por el contrario- no se dirige al mismo fin del autor mediato sino a uno distinto cualquiera. El dolo del instrumento faltará siempre que este obre con error o ignorancia sobre las circunstancias del tipo'. En efecto, es cierto que la percepción de fondos ajenos en sus cuentas bancarias personales, el posterior extracto del sistema bancario y, en algunos casos, el giro de ese dinero al exterior fueron voluntarios y conscientes, pero ello bajo la creencia de que actuaban legítimamente en razón del supuesto contrato de trabajo suscripto con empresas internacionales con las que se contactaron a través de internet, las que impartían las directivas prometiendo a cambio remuneración*".[(34)]

d) *Scamming*

Los actos de *scamming* se llevan a cabo a través de correos electrónicos fraudulentos, que pretenden estafar económicamente por medio del engaño. Comúnmente ofrecen oportunidades de viajes, premios, préstamos, donaciones, lotería, ofertas, promociones, cursos y becas. De esta manera, logran convencer ilícitamente a un usuario para proporcionar sus datos personales, lugar de residencia, número de teléfono, cuentas bancarias, etc. Consiste en una variedad de estafas vía internet, entre las que podemos mencionar las siguientes: a) oportunidad de cobro de una suma de dinero en algún país lejano como resultado de una resolución judicial; b) una persona "amiga" en el extranjero lo refirió para el sorteo de un viaje en crucero por una semana, para dos personas; c) préstamos de dinero o refinanciamiento de deudas a muy bajo interés; d) comunicación de haber ganado un premio en una lotería; e) apelar al dolor humano para contribuir a una causa noble (puede estar combinado con el *phishing)*; f) venta de software por Internet, supuestamente legal y licenciado[(35)]; y g) ofrecimiento laboral fraudulento.

(34) "P. y otros s/defraudación" - CNCrim. y Correc. - Sala V - 24/10/2013 - Cita digital IUSJU226163D

(35) Sumire, Helder C.: "Una breve reseña del delito informático" - ver en: scribd.com - pág. 15 - Consultado el 20/4/2018

e) *Spyware*

El spyware se presenta como pequeños programas que se instalan en el sistema o computadora, con la finalidad de rastrear nuestros datos y espiar nuestros movimientos por la red. Después envían esa información a otro servidor para fines ilícitos. Se instalan cuando: a) al visitar sitios de Internet que nos descargan su código malicioso (ActiveX, JavaScrips o Cookies) sin nuestro consentimiento; b) acompañado de algún virus o llamado "Troyano"; y c) están ocultos en un programa gratuito (Freeware), los cuales al aceptar sus condiciones de uso permiten el espionaje.(36)

f) *Skimming*

Son dispositivos colocados en los cajeros, monederos electrónicos, saldomáticos, *pin pads*, POS, *skimmers*, puertas de acceso, etc. Su objetivo es copiar en forma fraudulenta la banda magnética y el PIN de una tarjeta electrónica y luego la clonan o copian.(37)

g) Cardado

El cardado es un registro que utilizan los *skimmers* o clonadores vía internet o cajeros automáticos. Buscan verificar el saldo de las tarjetas electrónicas clonadas, mediante compras con montos pequeños para que el usuario o cliente no se alerte por la pérdida, retiro o transferencia.(38)

h) *Numerati*

El *numerati* es un correo electrónico o programa aplicativo que se descarga en el servidor para rastrear nuestros movimientos por la red. Luego se comercializan a empresas de servicios, publicidad o estadística. De este modo se disuade a los usuarios de visitar sitios o páginas web redireccionadas, con fines comerciales.(39)

i) Virus informáticos

Los virus informáticos son ataques destructivos, son realizados totalmente a través de las computadoras y en casos especiales con la complicidad de terceros, en forma fisica en determinadas eventualidades, de los cuales podemos citar los siguientes: 1. la propagación de virus informáticos destructivos; 2. envío masivo de correo no deseado o SPAM; 3. suplantación de los remitentes de mensajes con la técnica *spoofing*; 4. envío o ingreso subrepticio de archivos o *keyloggers*; 5. uso de Troyanos/*Backdoors* para el control remoto de los sistemas o la sustracción de información; 6. uso de archivos BOT del IRC y *Rootkits*

(36) Sumire, Helder C.: "Una breve reseña del delito informático"- ver en: scribd.com - pág. 16 - Consultado el 20/4/2018

(37) Sumire, Helder C.: "Una breve reseña del delito informático" - ver en: scribd.com - pág. 18 - Consultado el 20/4/2018

(38) Sumire, Helder C.: "Una breve reseña del delito informático" - ver en: scribd.com - pág. 18 - Consultado el 20/4/2018

(39) Sumire, Helder C.: "Una breve reseña del delito informático" - ver en: scribd.com - pág. 18 - Consultado el 20/4/2018

para el control remoto de sistemas, sustracción de información y daños irreversibles; y 7. ataques a servidores con el objeto de sabotearlos.(40)

j) Robo, usurpación o suplantación de identidad

El robo, la usurpación o suplantación de identidad es un tema muy relevante. A través de él los delincuentes utilizan datos personales para hacerse pasar por el individuo al que le han robado su identidad. Estos robos, en combinación con el anonimato de las transacciones en línea y otras actividades, se utilizan para cometer una serie de delitos que comprenden desde el fraude hasta las actividades terroristas. Dentro de esta modalidad se encuentra el fraude bancario, la extorsión en línea, el blanqueo de dinero y el contrabando con ayuda de computadoras y los delitos contra sistemas de computación y sus usuarios, con utilización de virus y otros programas hostiles, así como ataques de denegación de servicios.(41)

Este delito se caracteriza por la apropiación de la identidad de una persona, haciéndose pasar por ella y se lleva a cabo a través de la pérdida, robo o fotocopiado del DNI. También lo pueden hacer con datos personales que obtienen de distintos lugares. En forma virtual se usan las técnicas de la ingeniería social o la introducción de software malicioso en la computadora de la víctima.(42)

El delito suele ser una situación muy traumática para la víctima, pues en el sistema financiero puede verse envuelta en una serie de circunstancias no provocadas por ella y que desconoce, como que hayan obtenido en su nombre otorgamientos de créditos, tarjetas de crédito, cuentas corrientes -con sus consecuentes libramientos de cheques sin fondos-, intimaciones de pago, embargos, cierres de cuentas corrientes existentes, inhabilitación para operar con cuentas en el Banco Central de la República Argentina (BCRA), que se encuentre con datos negativos de deudas morosas en las empresas de informes crediticios y en la Central de Deudores del BCRA, entre otras circunstancias.

El robo de identidad no se encuentra tipificado en nuestro ordenamiento jurídico penal como un delito específico, sino que se encuentra dentro de las defraudaciones en general. Se han presentado algunos proyectos de ley al Parlamento para incorporarlo al CP, pero hasta la fecha no han prosperado.

Como mero ejemplo podemos citar los alcances en el caso "Serradilla"(43), donde el actor de la causa había tramitado el triplicado de su DNI ante el Registro Nacional de las Personas de Mendoza, el que, a pesar de haber sido reclamado en numerosas ocasiones, nunca le fue entregado al actor. Así fue hasta que del "*banco de Boston, del cual era cliente y único banco con el que operaba, le informó que a raíz de la comunicación del BCRA que había resuelto inhabilitarlo para operar en cuenta corriente en todo el país por librar cheques sin provisión de fondos, procedería a cerrar su cuenta y a dar de baja las tarjetas de crédito que le habían sido otorgadas por la institución, lo que finalmente ocurrió pocos días*

(40) Sumire, Helder C.: "Una breve reseña del delito informático" - ver en: scribd.com - pág. 16 - Consultado el 20/4/2018

(41) Altmark, Daniel R. y Molina Quiroga, Eduardo: "Tratado de derecho informático" - LL - Bs. As. - 2012 - T. I - págs. 271/2

(42) Fernández Delpech, Horacio: "Manual de derecho informático" - Ed. AbeledoPerrot - Bs. As. - 2014 - pág. 222

(43) "Serradilla, Raúl Alberto c/Mendoza, Provincia de y otro s/daños y perjuicios" - CSJN - 12/6/2007, S. 2790. XXXVIII

después". Relata la víctima que concurrió a la delegación de Organización Veraz de Mendoza, donde obtuvo datos de pedidos de informes sobre su situación patrimonial de distintos bancos. Se presentó ante tales bancos y detectó que en dos de ellos había cuentas abiertas a su nombre y al exhibírsele una fotocopia del DNI triplicado (el que nunca le había sido entregado) con sus datos personales observó que la fotografía, la firma y la impresión del dígito pulgar no se correspondían con las de él. Ante tales circunstancias, promovió una denuncia penal y luego la acción civil por daños y perjuicios.

Consecuentemente con este precedente, en el caso "Monaldo, Daniel Alfonso c/Banco Central de la República Argentina y otros s/daños y perjuicios" surge que *"tal como resulta de la prueba producida, el aquí accionante resultó víctima de una maniobra delictiva de uso de documento público apócrifo destinado a acreditar la identidad de personas, en cuyo marco se fraguó la toma de un crédito en el entonces Banco Velox, todo lo cual fue así declarado por sentencia dictada por el Tribunal Oral Federal N° 4, el cual ordenó al Banco Central de la República Argentina que eliminase al actor de autos de la nómina de deudores por la deuda originada en el uso de una tarjeta de crédito emitida por el Banco Velox, debiendo comunicar dicha exclusión al Banco Velox y a las empresas Veraz y Fidelitas*".[44]

Con el propósito de que puedan tomarse algunos recaudos en relación con la usurpación de identidad, la Dirección Nacional de Protección de Datos Personales, a través de la disposición 10/2010[45], creó el Registro Nacional de Documentos de Identidad Cuestionados. Su objetivo es organizar y mantener actualizado un registro informatizado donde consten el número y tipo de documentos de identidad que hayan sido denunciados por las autoridades públicas competentes y/o sus titulares, con motivo de pérdida, hurto, robo o cualquier otra alteración.

Solo debe considerarse la información positiva, la cual revela que el documento solicitado se encuentra inscripto con algún tipo de cuestionamiento ante el Registro Nacional de Documentos de Identidad Cuestionados. Un resultado negativo implica que el documento consultado no se encuentra informado ante el mencionado Registro.

V - REFLEXIONES RELATIVAS A LA RESPONSABILIDAD CIVIL POR LOS DAÑOS OCASIONADOS POR LOS DELITOS FINANCIEROS

En la responsabilidad que genere el deber de indemnizar deben configurarse los presupuestos de procedencia exigidos por nuestro ordenamiento jurídico, es decir, una conducta ilícita o antijurídica, un daño, la relación de causalidad entre el daño y el hecho generador del mismo, y un factor de atribución de responsabilidad. Estos factores de responsabilidad pueden ser subjetivos -cuando la atribución de responsabilidad es la culpa que consiste en la omisión de la diligencia debida, según la naturaleza de la obligación y las circunstancias de las personas, el tiempo y lugar; comprende la imprudencia, la negligencia y la impericia en el arte o profesión-; también será subjetiva cuando la atribución de responsabilidad es el dolo, el que se configura por la producción de un daño de manera intencional o con manifiesta indiferencia por los intereses ajenos (art. 1724, CCyCo.) y será objetiva cuando el daño causado provenga del "*riesgo o vicio de*

(44) "Monaldo, Daniel Alfonso c/Banco Central de la República Argentina y otros s/daños y perjuicios" - CNFed. Cont. Adm. - Sala III - 30/10/2009 - Cita digital IUSJU050079C

(45) Agencia de Acceso a la Información Pública. Jus.gob.ar (consultado 14/5/2018)

las cosas, o de las actividades que sean riesgosas o peligrosas por su naturaleza, por los medios empleados o por las circunstancias de su realización" (art. 1757, CCyCo.). Responde quien la realiza, se sirve u obtiene provecho de ella, por sí o por terceros, excepto lo dispuesto por la legislación especial (art. 1758).[46]

En tal sentido, la CSJN ha expresado en el caso "Serradilla" comentado en el apartado anterior que "*dicha responsabilidad no obsta a la que, frente a la característica de obligaciones concurrentes que se presenta, corresponde adjudicar a los estados nacional y provincial por la deficiente prestación del servicio a su cargo ante la demostración de la adecuada relación causal existente entre la conducta imputada y el resultado dañoso ocasionado*".[47]

Resulta relevante la atribución de responsabilidad objetiva que se le endilga a los bancos en el fallo "Bieniauskas, Carlos c/Banco de la Ciudad de Buenos Aires s/ordinario" por los daños ocasionados a la víctima en un caso de *phishing*. El Tribunal actuante entendió "*evidente que el sistema (*software *y* hardware*) que permite operar una red de cajeros automáticos puede ser calificado de cosa riesgosa. En rigor esta calificación puede ser asignada, en este punto al sistema informático que opera las transacciones remotas, sea mediante el denominado* home banking *sea por el uso de cajeros automáticos*". Y agrega: "*Todos estos elementos, que revelan una reingeniería en la prestación de los servicios bancarios un incipiente pero constante cambio cultural hacia el uso de medios informáticos, son trascendentes para interpretar la conducta de las partes y la responsabilidad que sigue frente a un hecho irregular como el aquí analizado. Cabe reparar que el Banco al ofrecer a sus clientes un nuevo modo de relacionarse con él, debe procurar como mínimo, brindarle igual seguridad que si tal operatoria se realizara personalmente*". Además sostiene "*la posibilidad técnica de 'duplicar' las tarjetas no solo revela la falibilidad del sistema, y nuevamente su calidad de cosa riesgosa, sino también la irrelevancia de la conducta del actor en el punto*". Asimismo afirma la atribución de responsabilidad objetiva expresando "*sea que se invoque la ley de defensa del consumidor (*art. 40, ley 24240*), como de aplicarse el código civil (*art. 1113*), se arribará a igual resultado: asignar al Banco responsabilidad por lo ocurrido en tanto ambos supuestos prevén un sistema objetivo en esa materia*".[48]

Otro caso donde podemos resaltar la imputabilidad de la responsabilidad a las entidades financieras lo observamos en la causa "Díaz, Luciana Paula c/Compañía Financiera Argentina SA y otro s/ordinario" sobre robo de identidad. El Tribunal ha manifestado que "*como ha sido reiteradamente sostenido por la jurisprudencia, es obligación del banco extremar los recaudos tendientes a verificar la identidad de las personas con quienes contrata. De ahí que, comprobado -como ha sido en el caso- que el préstamo de marras fue otorgado a una persona que fraguó la identidad de la actora, haciéndose pasar por esta, algo es claro: el resultado que debía alcanzarse -esto es, que el préstamo respectivo no fuera canalizado bajo una falsa identidad- no se logró*". Y agrega: "*En tales condiciones, no es posible aceptar, como pretende la recurrente, que su parte haya*

(46) Martínez, Matilde S.: "Algunas cuestiones sobre responsabilidad por la inclusión inadecuada de los datos de carácter personal en los informes crediticios" - Ed. AbeledoPerrot - Nº: AP/DOC/964/2017 - 29/11/2017

(47) "Serradilla, Raúl Alberto c/Mendoza, Provincia de y otro s/daños y perjuicios" - CSJN - 12/6/2007, S. 2790. XXXVIII

(48) "Bieniauskas, Carlos c/Banco de la Ciudad de Buenos Aires s/ordinario" - CNCom. - Sala D - 1/7/2008 - Cita digital IUSJU058123C

arbitrado todas las diligencias a su alcance para evitar esa pretendida estafa, máxime cuando, en su calidad de sociedad esencialmente profesional y empresaria, la demandada se encontraba sujeta a estándares de conducta mucho más severos que los que deben ser aplicados al común de las gentes". Además sostiene: "*A estas circunstancias fácticas se agrega otra, esta vez de índole jurídica, que me habilita a concluir que la demandada debe responder por los daños que la actora sufrió a causa del episodio de marras. Me refiero al hecho de que la actora debe considerarse 'consumidora' en los términos de los arts. 1 y 2 de la ley 24240, texto según la ley 26361; ley que, por ende, deviene aplicable al caso e impone la solución anticipada*".[49]

VI - CONCLUSIÓN

Hemos analizado desde la aparición de la era informática hasta los delitos más comunes que se cometen a través del fenómeno de las nuevas tecnologías de la información y la comunicación, en especial en el ámbito financiero y bancario. Además analizamos cuestiones sobre la responsabilidad civil por las consecuencias dañosas que se ocasionan a las víctimas de estos delitos, para concluir resaltando la importancia de los sistemas de seguridad que se deben emplear como recaudos para minimizar las vulnerabilidades de los sistemas informáticos y los consecuentes daños que producen los ataques de los ciberdelincuentes, tanto a los usuarios como a las entidades financieras.

En relación con ello, el BCRA, a través de la Comunicación "A" 5374[50], ha dictado las normas sobre los "*requisitos mínimos de gestión, implementación y control de los riesgos relacionados con tecnología informática, sistemas de información y recursos asociados para la entidades financieras*", alcanzando a las operaciones a través de cajeros automáticos, terminales de autoservicio, banca móvil, banca telefónica, banca por internet y puntos de venta. En esta norma se establecen los requisitos mínimos de seguridad que deben implementar las entidades financieras. No obstante ello, estas deben disponer de todas aquellas medidas de seguridad adicionales para realizar una eficiente gestión de riesgos en las operaciones dinerarias con sus clientes.

(49) "Díaz, Luciana Paula c/Compañía Financiera Argentina SA y otro s/ordinario" - CNCom. - Sala C - 15/12/2016 - Cita digital IUSJU014216E

(50) Com. 5374. t.o. vigente desde 1/3/2013. BCRA. Consultado el 16/5/2018

Delitos informáticos y cibercrimen: alcances, conceptos y características

Marcelo Temperini(*)

I - INTRODUCCIÓN

En los tiempos en que se redacta este artículo ya no correspondería afirmar que los delitos informáticos son un "nuevo fenómeno", al menos socialmente. Sí podríamos aceptar que es algo "nuevo" para el derecho, y para el derecho penal en particular, al menos en relación con el desarrollo doctrinario histórico de esta materia.

La delincuencia informática o ciberdelincuencia ya lleva varios años de gestación, desarrollo y sobre todo de mucha práctica, bastante lucrativa para los delincuentes.

Si bien hace años que los delitos informáticos forman parte de la delincuencia en nuestra sociedad, no deja de sorprender que en la última década el índice de ciberdelincuencia haya aumentado notoriamente; quizás, es una problemática que, a los ojos del ciudadano común, se ha hecho cada vez más visible.

El inexorable paso del tiempo, en combinación con otros aspectos (como el aumento de la dependencia de las personas de las tecnologías de la información), se encarga de generar los incidentes de seguridad de la información que hacen que el ciudadano común vaya tomando conocimiento y dimensión de la existencia de este tipo de delitos (que para él sí son "nuevos").

En este aspecto, algunos casos mediáticos han sido útiles para dar a conocer los distintos riesgos que implican la utilización de las redes de información. Casos como los

(*) Abogado (UNL). Especialista en derecho informático y ciberdelincuencia. Doctorando dedicado a la investigación de delitos informáticos y cibercrimen (FCJS/UNL). Socio Fundador de AsegurarTe Cofundador del Proyecto ODILA: Observatorio de delitos informáticos de Latinoamérica. Miembro de la Comisión Directiva de ADIAr

cables diplomáticos y secretos difundidos por Wikileaks[1], la aparición en la escena mundial de Edward Snowden[2] y la apertura al mundo del programa de espionaje PRISM por parte de Estados Unidos, el ciberataque mundial más grande que logró dejar sin sistemas a grandes multinacionales como Telefónica[3], junto con otros tantos casos en Latinoamérica y Argentina[4][5] visibilizan cada vez más la existencia del fenómeno de la ciberdelincuencia en la sociedad, cada vez más numerosa y organizada.

Este artículo pretende explicar la complejidad que representa un abordaje profundo de un tema tan importante como la ciberdelincuencia. En esta ocasión, buscaremos realizar un repaso de algunos aspectos de la seguridad de la información, que consideramos son imprescindibles al momento de comprender los argumentos a partir de los cuales giran los delitos informáticos. Luego introduciremos distintos conceptos tradicionales de la doctrina sobre delitos informáticos y cibercrimen, sus características generales y los desafíos que representan para el derecho.

II - ASPECTOS BÁSICOS DE LA SEGURIDAD DE LA INFORMACIÓN

El aumento en la cantidad de incidentes de seguridad es significativo y desde el punto de vista de la seguridad de la información es hasta lógico que así ocurra. Según el Lic. Cristian Borghello[6], para comenzar el análisis de la seguridad informática se deberán conocer las características de lo que se pretende proteger: la información.

El citado autor sostiene[7] que la información "*Es una agregación de datos que tiene un significado específico más allá de cada uno de estos*". Tendrá un sentido particular segun cómo y quién la procese. Por ejemplo, 1, 9, 8 y 7 son datos; su agregación 1987 es información.

En palabras del Lic. Cristian Borghello, "*Establecer el valor de la información es algo totalmente relativo, pues constituye un recurso que, en muchos casos, no se valora adecuadamente debido a su intangibilidad, cosa que no ocurre con los equipos, las aplicaciones y la documentación*".

En este sentido, consideraremos como incidente de seguridad a todos los hechos no deseados donde se comprometa de cualquier forma la seguridad de la información. Es decir, todos los delitos informáticos son, en el fondo, incidentes de seguridad de la información.

(1) "La Casa Blanca implora a WikiLeaks que no filtre más documentos sobre la guerra" - Diario Clarín - 30/7/2010. Ver en: clarin.com. Consultado el 27/11/2013

(2) "Hackeamos a cualquiera en cualquier parte del mundo" - Diario Clarín - 11/6/2013. Ver en: clarin.com. Consultado el 27/11/2013

(3) "El masivo ciberataque ya afectó a 99 países e incluyó casi 150.000 incidentes" - Diario Clarín - 12/5/2017. Ver en: clarin.com. Consultado el 20/5/2017

(4) "También hackearon 30 correos del Ministerio de Seguridad" - Diario La Nación - 1/2/2017. Ver en: lanacion.com.ar. Consultado el 20/5/2017

(5) "Denuncian que un hacker se robó $ 3.500.000 de una cuenta municipal" - Diario Clarín - 23/11/2016. Ver en: www.clarin.com. Consultado el 20/5/2017

(6) Borghello, Cristian F.: "Seguridad informática. Su implicancia e implementación" - 2001 - Reg.UTN/Facultad 0015/793

(7) Fernández Calvo, Rafael: "Glosario Básico Inglés-Español para usuarios de Internet" - 1994-2000. Ver en: ati.es. Consultado el 14 de Julio de 2016

Tengamos en cuenta que estamos utilizando la palabra "información" y no "informática" toda vez que esta disciplina (seguridad de la información) pretende abordar y trabajar por el aseguramiento de la información, independientemente del medio en el cual la misma sea almacenada o tratada. Es decir que aplica tanto para la información en bases de datos informatizadas como para los ficheros en papel que tiene cualquier médico de la ciudad.

Volviendo al punto anterior, todo incidente de seguridad puede ser estudiando -o debería- para determinar sus orígenes y, en consecuencia, poder trabajar sobre los diferentes riesgos que dieron lugar al mismo. Los científicos de esta disciplina están en su mayoría de acuerdo en afirmar que los riesgos pueden ser de cuatro categorías: negados, reducidos, asumidos o transferidos. Entre ellos, lo que no debería suceder es negar la existencia de los riesgos, o, al menos, es lo menos saludable para cualquier organización. La reducción o mitigación del riesgo es lo más normal o común de encontrar, e implica la adopción de diferentes medidas de seguridad que aportan a la disminución del riesgo -*tengamos en cuenta que nunca el riesgo podrá llevarse al mínimo, toda vez que no existe la seguridad absoluta*-.

Las otras opciones implican, por un lado, asumir el riesgo, es decir que el responsable de la información sabe que existe y acepta someterse a la eventual ocurrencia de esos incidentes de seguridad; por el otro, la última opción, la transferencia del riesgo, implica precisamente que un tercero pasa a asumir la responsabilidad en el caso de la ocurrencia del mismo -similar a lo que sucede con la contratación de cualquier póliza de seguros-. Es decir, asumo que existe el riesgo de chocar, pero ante esa eventualidad, estaré cubierto por un tercero que se hará "responsable" por los daños ocasionados.

Adentrándonos un poco más en el mundo de la seguridad de la información, y aquí sí con mayor conexión hacia el tema madre de este trabajo, diremos que existen tres pilares básicos que se buscan o intentan resguardar: confidencialidad, integridad y disponibilidad. Si bien algunos autores agregan otros pilares extras, todos coinciden en que estos tres son los básicos.

Nuevamente recurriremos al trabajo del Lic. Cristian Borghello[8], para citar sus definiciones sobre estos tres pilares:

- La integridad de la información es la característica que hace que su contenido permanezca inalterado, a menos que sea modificado por personal autorizado, y esta modificación sea registrada para posteriores controles o auditorias. Una falla de integridad puede estar dada por anomalías en el *hardware*, *software,* virus informáticos y/o modificación por personas que se infiltran en el sistema.
- La disponibilidad u operatividad de la información es su capacidad de estar siempre disponible para ser procesada por las personas autorizadas. Esto requiere que la información se mantenga correctamente almacenada, con el *hardware* y el *software* funcionando perfectamente y que se respeten los formatos para su recuperación en forma satisfactoria.
- La privacidad o confidencialidad de la información es la necesidad de que la misma solo sea conocida por personas autorizadas. En casos de falta de confidencialidad, la información puede provocar severos perjuicios a su dueño (por ejemplo, conocer antecedentes médicos de una persona) o volverse obsoleta (por ejemplo, los planes de

(8) Borghello, Cristian F.: Tesis "Seguridad Informática. Su implicancia e implementación" - 2001, Reg.UTN/Facultad 0015/793

desarrollo de un producto que se "filtran" a una empresa competidora facilitarán a esta última desarrollar un producto de características semejantes).

Dejamos aquí nuestro desarrollo en materia de seguridad de la información, prometiendo al lector recuperar estos conceptos y destacar la importancia de estos tres pilares en nuestro estudio sobre los delitos informáticos.

III - LAS NUEVAS TECNOLOGÍAS COMO POTENCIADORAS DEL DELITO

Cuando comenzamos este trabajo, adelantamos que ya no es posible afirmar que los delitos informáticos son algo novedoso o un fenómeno al cual deberíamos mostrarnos con asombro. Al menos no debería ser así para aquellos que se encuentran cercanos al mundo de la tecnología o, incluso, vinculados al ámbito del derecho penal.

A lo largo de la historia, el delito ha encontrado en la tecnología un aliado, toda vez que los delincuentes siempre han buscado innovar utilizando las herramientas y tecnología a su alcance para lograr sus objetivos.

No pretendemos aquí hacer un desarrollo exhaustivo sobre el delito en sí -tarea que escapa al alcance de este trabajo- pero a los fines de nuestros objetivos, y como operadores del derecho (otras ciencias como la criminología tienen otros conceptos), denominaremos "delito" a toda acción que así sea dispuesta por ley. Más concretamente, entenderemos como delito toda acción típica, antijurídica y culpable, siguiendo la doctrina clásica[9] del derecho penal.

Debe advertir el lector que en el tema de estudio es muy común encontrar textos, artículos, libros y especialistas que se refieren a "delitos informáticos" y muchas veces se incluyen conductas que, al menos en Argentina, no se encuentran tipificadas penalmente. Entiendo que dicha situación es consecuencia de varios factores, esencialmente de la existencia en el ambiente de muchos profesionales de las ciencias informáticas, particularmente del ámbito de la seguridad de la información. Su concepto de delito no es estrictamente penal, por lo que la utilización de dicho concepto en el marco de artículos y conferencias de seguridad de la información puede generar confusiones a aquellos acostumbrados a entender su concepto jurídico.

Adicionalmente debemos mencionar la dificultad de abordar la temática desde una óptica nacional, ya que, como hemos visto anteriormente, los delitos informáticos -como todo fenómeno relacionado con las nuevas tecnologías- son una problemática de índole internacional o general, donde los límites jurisdiccionales "clásicos" del derecho suelen tornarse cada vez más borrosos.

Realizada esta pequeña digresión, intentaremos argumentar nuestra opinión acerca del entendimiento de que las nuevas tecnologías son "potenciadoras de los delitos". No será necesario explicar los numerosos aspectos positivos que las nuevas tecnologías han brindado a la vida de las personas, como la posibilidad de la comunicación instantánea, el contacto a distancia, la posibilidad de teletrabajo, acceso a la información, entre una serie de grandes beneficios que no pretendemos aquí desarrollar.

Entre todas las características que podrían desarrollarse sobre las tecnologías de la información y la comunicación (TIC), nos concentraremos en tres: 1. la inmediatez de las comunicaciones a distancia, 2. la posibilidad de la realización de acciones masivas

(9) Creus, Carlos: "Derecho Penal: Parte General" - 5ª ed. actualizada y ampliada - Ed. Astrea - 2010

(automatizadas o no) y 3. la posibilidad de realizar acciones con un determinado nivel de anonimato.

Estas tres características de las nuevas tecnologías son las que desde nuestro punto de vista -y en combinación con una serie de factores que más adelante desarrollaremos- son la materia prima necesaria para generar el efecto potenciador de los delitos.

Muchos de los delitos informáticos más comunes -estafas, injurias, amenazas y hasta la propia distribución de pornografía infantil- existen desde mucho antes que existiera internet. Sin embargo, la combinación de la tecnología con muchos de estos delitos terminan dando lugar a una nueva versión de los mismos, a un nuevo nivel en la forma de comisión de estos delitos que viene posibilitada de la mano de las características propias de las nuevas tecnologías que anteriormente citábamos (inmediatez a distancia, masividad y anonimato). Por ejemplo, un estafador clásico debía tomar sus recaudos en el tipo de engaño, acercarse a la víctima, teniendo las habilidades sociales necesarias, hacer incurrir en el error a la víctima y, así, lograr llevar adelante una estafa. Todos estos pasos resultan casi automatizados en las estafas electrónicas, donde las posibilidades de éxito del delincuente aumentan radicalmente. A través de las herramientas tecnológicas, desde cualquier lugar con conexión a Internet (realización a distancia), el delincuente podrá atacar múltiples víctimas a la vez (masividad), enviando cientos de correos electrónicos a la vez, de forma instantánea (no se necesita esperar), y, de acuerdo al nivel de conocimiento del delincuente, hasta podrá utilizar determinados mecanismos que obstaculicen su rastreo o identificación (anonimato).

Estos mismos pasos podríamos citarlos en el caso del delito de distribución de pornografía infantil. Hasta hace algunos años, los dueños de este tipo de material debían revelar sus propias fotos, enviárselas a otras personas a través del correo postal o hacer intercambios personales. Actualmente, todo eso es facilitado por las nuevas tecnologías, donde esta clase de delincuentes se encuentran con mayores posibilidades de continuar sus acciones delictivas.

Desde este punto de vista, las tecnologías son potenciadoras de determinados tipos de delitos, que no son nuevos sino clásicos, pero que, al combinarse con las características de las nuevas tecnologías de la información, terminan llevando el delito a un nuevo nivel de desarrollo. Se observa un aumento inusitado en la cantidad de sujetos pasivos, debido a que -a diferencia de la inseguridad clásica- ya no importan el barrio, el apellido, la ropa o si lleva un arma de protección, todos los usuarios conectados a internet se convierten en potenciales víctimas.

La masividad de la difusión de los contenidos también puede generar que en determinados tipos de delitos (como injurias, calumnias, etc.), el daño producido se vea enormemente potenciado. Pensemos como ejemplo los casos de difusión no consentida de imágenes íntimas, que antes de Internet podían llegar como mucho a ser publicadas en alguna revista de moda (que eventualmente también sería responsable). En la actualidad, la viralización de un contenido aumenta exponencialmente el daño producido a la persona afectada, incluso en canales como Whatsapp, donde ni siquiera es posible detener o al menos saber en cuántos dispositivos alrededor del mundo se encuentra una imagen.

Por último, la utilización de herramientas de anonimización utilizadas por los ciberdelincuentes, en combinación con las dificultades propias para la determinación de la autoría en internet, terminan complejizando arduamente las tareas de investigación de las fuerzas de seguridad y los organismos competentes, que se ven compelidas a realizar una actualización y capacitación constante para poder hacer frente a este tipo de delitos.

Como cierre de esta sección, y para evitar dejar un sabor amargo en la retina del lector, creemos necesaria una reflexión sobre la neutralidad de la tecnología en general, y de las nuevas TIC en particular, para no caer en la condena o estigmatización de las nuevas tecnologías. Por un lado, afirmamos nuestra posición acerca de considerar que todas las tecnologías son neutras. Es decir que no son buenas ni malas en sí mismas, sino que ello dependerá de la intención de la persona que las utiliza. Por otro, comprender que así como disfrutramos a diario los incontables beneficios que podríamos citar dentro de los aspectos positivos, también debemos -socialmente- hacernos cargo de todas aquellas acciones negativas posibles, entre las que encontramos muchos de los delitos que constituyen el objeto de este artículo.

IV - DELITOS INFORMÁTICOS. CONCEPTOS Y ALCANCES

Para poder seguir avanzando en este trabajo, es necesario hacer aquí un punto de partida conceptual sobre el término "delito informático", con el propósito de poder negociar con el lector un denominador común sobre su definición y, sobre todo, de su alcance.

Inicialmente debemos reconocer la inexistencia de un acuerdo en la doctrina acerca de su definición, así como la inexistencia de una norma (al menos en Argentina) que establezca algún tipo de partida para aceptar o criticar jurídicamente su concepto.

De acuerdo con el maestro Dr. Julio Téllez Valdés[10], estos delitos se pueden clasificar en sus formas típica y atípica, entendiendo por la primera a "*las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin*" y por las segundas a "*actitudes ilícitas en que se tienen a las computadoras como instrumento o fin*". Si bien existen otros tantos conceptos en la doctrina, se toma el citado toda vez que su simple clasificación entre típicos y atípicos es útil para nuestros fines. Aquí solamente se consideran como "delito informático" a aquellos dentro de la categoría de los "típicos", es decir, como una conducta penalmente sancionada por un país determinado.

La Organización para la Cooperación Económica y el Desarrollo define al "delito informático" como "*Cualquier conducta, no ética, o no autorizada, que involucra el procesamiento automático de datos y/o la transmisión de datos*"[11]. Jijena Leiva los define como: "*…toda acción típica, antijurídica y culpable, para cuya consumación se usa la tecnología computacional o se afecta a la información contenida en un sistema de tratamiento automatizado de la misma*".[12]

El Dr. Alexander Díaz García[13] considera que los delitos informáticos deben ser observados desde un punto de vista triple: "*Como fin en sí mismo, pues el computador puede ser objeto de la ofensa, al manipular o dañar la información que este pudiera contener; Como medio: Como herramienta del delito, cuando el sujeto activo usa el ordenador para facilitar la comisión de un delito tradicional; Como objeto de prueba: Los computadores guardan pruebas incidentales de la comisión de ciertos actos delictivos a través de ellos*".

(10) Téllez Valdés, Julio: "Derecho informático" - 3ª ed. - Ed. Mc Graw Hill - México - 2003 - pág. 8

(11) OCDE: "Delitos de Informática: análisis de la normativa jurídica" - Ver en: ocde.org

(12) Jijena Leiva, Renato J.: "La criminalidad informática: Situación de *lege data* y *lege ferenda* en Chile" - Actas de III Congreso Iberoamericano de Informática y Derecho" - Mérida - España

(13) Diaz García, Alexander: "El bien jurídico tutelado de la información y los nuevos verbos rectores en los delitos informáticos" - Ver en: oas.org

En una subcategoría del propio concepto de delito informático se plantea una decisión que establece que, dependiendo de la postura adoptada, los delitos informáticos pueden tratarse de un puñado de tipos penales o bien estos pueden multiplicarse de una forma considerable.

Nos estamos refiriendo a que en algunos casos se decide utilizar el concepto de "delito informático" de forma reservada para aquellos tipos penales más específicos de la materia (por ejemplo, casos de *hacking, cracking,* denegación de servicios, *grooming*, etc.). Sin embargo, de acuerdo con una interpretación estrictamente jurídica del concepto ya desarrollado anteriormente, si la conducta típica se realiza a través de "medios informáticos" -lo que a nuestro criterio sería más correcto que decir que se realiza a través de computadoras, como expone originalmente el Dr. Julio Tellez- también pasaría a ser un delito informático.

¿Es correcta esta interpretación? El autor Miguel Á. Davara Rodríguez[14] define el delito informático como "*la realización de una acción, que reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software*". Agrega luego: "*Nos estamos refiriendo solamente, a la comisión de un delito por medios informáticos o telemáticos, ya que la comisión de otros delitos en los que alguna forma interviene un elemento informático, se encontrará sin duda dentro del Derecho Penal General*". Este autor parece darse cuenta de la importancia de definir cuál será el alcance que le daremos al concepto, y del riesgo que implicaría que cualquier participación menor de la tecnología en un delito termine por "convertirlo" en un delito informático.

En nuestra opinión, la respuesta es positiva y negativa a la vez. Es decir, en principio debe dejarse en claro que la mera intervención de un elemento informático no convierte a un delito clásico en un delito informático. Sin embargo, es necesario reconocer que, en determinados tipos penales, el ingrediente tecnológico es tan poderoso -de acuerdo a lo explicado sobre la potencialidad- que hace necesario que para su identificación, investigación y persecución intervengan especialistas dedicados a los delitos informáticos.

Es decir, hablamos de aquellos casos donde el tipo penal clásico es perfeccionado utilizando a las nuevas tecnologías como medio para su comisión, dotándolo de esa manera de muchos de los inconvenientes o desafíos clásicos de los delitos informáticos, tales como el anonimato, internacionalidad, dificultad en la obtención de evidencia digital, entre otros.

Podría legítimamente el lector preguntarse cuál sería la diferencia al juzgar que el delito sea considerado o no un delito informático, o si bien, se trata de una discusión meramente doctrinaria. En principio, la respuesta no parece ser tan importante toda vez que en Argentina -y a modo de adelanto- este tipo de delitos no generan una nueva categoría penal que pueda derivar en la aplicación o no de un régimen jurídico especial. No obstante, podría tornarse de interés a los fines de definir la jurisdicción y la competencia, recordando que en nuestro país ya empiezan a surgir las primeras fiscalías especializadas en ciberdelincuencia.[15]

(14) Davara Rodríguez, Miguel Á.: "Manual de Derecho Informático" - 10ª ed. - Ed. Thomson Aranzadi - págs. 358/59

(15) "Una fiscalía dedicada a los delitos informáticos" - Diario Clarín, Ver en: clarin.com. Consultada: 13/6/2017

V - CIBERCRIMEN Y CIBERDELINCUENCIA

Avanzando un poco más sobre el desarrollo de la temática, no podemos continuar sin abordar las diferencias entre el concepto de cibercrimen y ciberdelincuencia, o lo que sería lo mismo, entre delitos informáticos y cibercrimen, conceptos que normalmente son utilizados como sinónimos pero que a fines acádemicos y doctrinarios tienen diferencias que nos parece aquí el momento adecuado para señalarlas.

Principalmente la diferencia radica en la organización del delito. Es decir, cuando referimos a delitos informáticos, delincuencia informática o ciberdelincuencia, nos referimos a aquellos delitos que ocurren a diario, tipificados penalmente, pero que ocurren de forma independiente, o individual, sin encontrar elementos o indicios que nos permitan observar organización y regularidad en la comisión de la conducta en sí. Bastaría dar como ejemplo un caso de acceso indebido a una cuenta de correo electrónico, por ejemplo, realizado por una persona a su expareja. O bien, un empleado enojado que borra información importante (*inside job*) de la empresa a la que pertenece. Podríamos también mencionar (ya como delitos informáticos de segundo nivel), una amenaza de muerte realizada vía correo electrónico o Whatsapp. O las injurias o caluminas realizadas desde un perfil falso de Facebook. El denominador común de todos los casos mencionados es que los delitos existen y ocurren pero se cometen o llevan a cabo de forma aislada o independiente.

En cambio, cuando referimos al cibercrimen, estamos hablando de una serie de delitos informáticos que ocurren de una forma más profesional, organizada, sin motivaciones personales más que las económicas, donde los sujetos pasivos de los delitos son elementos funjibles y sin interés para el ciberdelincuente, que busca optimizar sus ganacias a través del perfeccionamiento de distintas técnicas delictivas que utilizan a la tecnología como eje. Si bien es posible encontrar ciberdelincuentes especializados que trabajan de forma independiente, es mucho más común encontrarlos organizados en bandas, con una clara distribución de tareas.

Como ejemplo en casos de cibercrimen podemos mencionar el *ransomware*, un tipo de *malware* (*software* malintencionado) que tiene como objetivo bloquear -cifrando- el acceso a toda o parte de la información que contiene el equipo, para después poder pedir un rescate a cambio de su liberación. Estos casos son ejemplos donde los ciberdelincuentes no están interesados en el objetivo o en la víctima, en su información en particular, sino que se realiza de forma masiva, buscando un fin de lucro, que es el pago por el rescate. Es un negocio organizado, donde las bandas suelen estar compuestas por personas que se dedican a desarrollar el *malware*, otras a infectar sistemas, otras a la "atención al cliente" vía foros o correo electrónico -donde se indican cuánto y cómo se debe pagar el rescate-, hay personas dedicadas a la gestión de las billeteras virtuales (que no duran más que unos días), otras al blanqueo del dinero y, por supuesto, hay líderes.

Similar ejemplo pero quizás con menor organización que esas nuevas bandas, y que siguen siendo un caso clásico de cibercrimen, son las dedicadas a las estafas electrónicas. Aquí nuevamente podremos encontrar bandas dedicadas a la captación ilegítima de datos confidenciales -datos de las tarjetas de crédito por ejemplo-, generalmente a través del *phishing*. El *phishing* es una técnica de ingeniería social utilizada por los delincuentes para obtener información confidencial, como nombres de usuario, contraseñas y detalles de tarjetas de crédito, haciéndose pasar por un contacto

confiable y legítimo[16]. En estas bandas podemos encontrar a los diseñadores de las páginas mellizas (que engañan a la víctima para que introduzca sus datos); los que se encargan de la distribución de los engaños vía *spam*, los encargados de recolectar y procesar los datos -y en algunos casos de venderlos en el mercado negro-; los que realizan las estafas propiamente dichas (ardid o engaño y un perjuicio patrimonial), comprando bienes o servicios con los datos robados; los encargados de blanquear el dinero, entre otra serie de tareas que se pueden econtrar. Nuevamente, vemos aquí un grupo de personas que hacen de estos delitos un oficio, donde pueden verse notas de organización y realización de forma masiva y continuada.

De acuerdo con un estudio realizado por una empresa de seguridad llamada Panda Security[17], las mafias de ciberdelincuentes que operan en internet están muy organizadas, tanto desde el punto de vista de visión estratégica como desde la operativa, logística y despliegue de sus operaciones. Y, además, no solo pueden parecer verdaderas compañías, sino que son organizaciones multinacionales, ya que operan a lo largo y ancho del planeta.

De este último informe, se ha extraído una clasificación, publicada por el FBI, de las diferentes "profesiones" del mundo de los cibercriminales, en un intento de tipificar las figuras más comunes que podemos encontrar en el proceso mafioso de generar dinero mediante el robo, la extorsión y el fraude a través de Internet.

Según el FBI, las organizaciones cibercriminales funcionan como empresas, y cuentan con expertos especializados para cada tipo de trabajo y ocupación. A diferencia de una organización empresarial, estos cibercriminales trabajan sin horarios, sin vacaciones y sin fines de semana. Las especializaciones más comunes que tipifica el FBI son las siguientes:

1. *Programadores. Desarrollan los exploits y el malware que se utiliza para cometer los cibercrímenes.*
2. *Distribuidores. Recopilan y venden los datos robados, actuando como intermediarios.*
3. *Técnicos expertos. Mantienen la infraestructura de la "compañía" criminal, incluyendo servidores, tecnologías de cifrado, bases de datos, etc.*
4. Hackers. *Buscan aplicaciones exploits y vulnerabilidades en sistemas y redes.*
5. *Defraudadores. Crean técnicas de ingeniería social y despliegan diferentes ataques de* phishing *o* spam*, entre otros.*
6. *Proveedores de* hosting. *Ofrecen un entorno seguro para alojar contenido ilícito en servidores y páginas.*
7. *Vendedores. Controlan las cuentas y los nombres de las víctimas y las proveen a otros criminales mediante un pago.*
8. *Muleros. Realizan las transferencias bancarias entre cuentas de banco.*
9. *Blanqueadores. Se ocupan de blanquear los beneficios.*
10. *Líderes de la organización. Frecuentemente, personas normales sin conocimientos técnicos que crean el equipo y definen los objetivos.*

(16) "*Phishing*" - Segu-Info. Ver en: segu-info.com.ar

(17) "El mercado negro del cibercrimen" - Panda Security - 2010. Ver en: prensa.pandasecurity.com - Consultado el 27/11/2013

Según este estudio, las organizaciones cibercriminales se organizan de forma jerárquica, y cada paso diferente de la cadena cuenta no con uno sino con varios especialistas.

Como anteriormente comentábamos, por lo general suele pensarse que los ciberdelincuentes informáticos actúan de forma aislada, espontánea, independiente, de acuerdo con distintas motivaciones. Sin embargo, el transcurso del tiempo y la acumulación de experiencia de los delincuentes trae consigo la existencia de redes organizadas dedicadas a la comisión de delitos cada vez más complejos, y la problemática está escalando en gravedad debido a la existencia de más redes internacionales dedicadas a este tipo de delitos.

Sobre estas bandas organizadas, y relacionado con el delito de distribución y comercialización de pornografía infantil a través de medios informáticos, se pueden citar en Argentina distintos casos de desbaratamientos de complejas redes. Este año, por ejemplo, a través de la denominada "Operación Oliver"[18], nacida bajo una investigación previa realizada en Londres, se realizaron 11 allanamientos en la ciudad de Buenos Aires, 24 en el conurbano bonaerense y 26 en distintas provincias (Salta, Tierra del Fuego, San Juan, Tucumán, Santa Fe, Santa Cruz, Córdoba, Santiago del Estero, Chaco, Entre Ríos y Neuquén), con la imputación de 64 personas involucradas.

VI - EL PROBLEMA DEL BIEN JURÍDICO PROTEGIDO

Un tema de gran importancia para la temática abordada es un adecuado razonamiento acerca de cuál es el bien jurídico protegido en los delitos informáticos. ¿Podría acaso ser el bien jurídico protegido el común denominador entre tantos delitos que a simple vista parecen tan distintos?

Podría decirse que la doctrina ha esbozado tantas definiciones del bien jurídico protegido como autores han tratado el tema. No en vano dijo Welzel[19] que "*el bien jurídico se ha convertido en un auténtico Proteo, que en las propias manos que creen sujetarlo se transforma en seguida en algo distinto*".

Por nuestra parte, y con la intención de partir de un concepto moderadamente aceptado, seguiremos a Von Liszt, quien sostiene que el "bien jurídico" puede ser definido como un "*interés vital para el desarrollo de los individuos de una sociedad determinada, que adquiere reconocimiento jurídico*".[20]

Superada la introducción conceptual, y siguiendo con la línea de desarrollo del artículo, existe un sector de la doctrina que opina que los delitos informáticos no son una nueva categoría, sino que simplemente son los mismos delitos de siempre cometidos a través de nuevos medios. En estos casos, este sector entenderá que los bienes jurídicos protegidos son los mismos de siempre, que simplemente se han actualizado los tipos

(18) Secretaría de Comunicación Pública de la Presidencia de la Nación: "La Policía Federal desarticuló una red internacional de pornografía infantil" - Ver en: prensa.argentina.ar - Consultado el 27/11/2013

(19) Welzel, ZStW, 58, párr. 491 ss., 509, cit. por Jakobs, Günther: "Derecho penal. Parte general. Fundamentos y teoría de la imputación" - trad. por Cuello Contreras, Joaquín y Serrano González de Murillo, José - 2ª ed. - Ed. Marcial Pons - Madrid - 1997 (2ª ed. alemana 1991) - págs. 47/8

(20) Von Liszt, Franz: "Tratado de derecho penal" - trad. de la 20ª ed. alemana por Jiménez de Asúa, Luis adicionado con el Derecho penal español por Quintilliano Saldaña - 4ª ed. - Ed. Reus - Madrid - 1999 - T. II

penales, incluyendo nuevos medios de comisión, como bien podría ser el caso de las modificaciones de los artículos 153 y 153 bis del Código Penal.[21]

Del otro lado de la balanza -como suele suceder en el derecho- existe una postura que considera que hay un nuevo bien jurídico que proteger que es la información, el cual tiene valor y debe ser puesto en la escena penal de forma independiente con respecto a otros bienes jurídicos. En palabras del Dr. Santiago Acurio Del Pino[22], "*Podemos decir que el bien jurídico protegido en general es la información, pero está considerada en diferentes formas, ya sea como un valor económico, como un valor intrínseco de la persona, por su fluidez y tráfico jurídico, y finalmente por los sistemas que la procesan o automatizan … Por tanto el bien jurídico protegido, acoge a la confidencialidad, integridad, disponibilidad de la información y de los sistemas informáticos donde esta se almacena o transfiere*".

Volviendo al aporte realizado por el jurista colombiano Díaz García, quien participó en el proyecto y posterior sanción de la ley que incorpora los delitos informáticos en Colombia, en dicha norma (*una de las más modernas de nuestro continente*), se considera a la información como bien jurídico protegido en el esquema penal colombiano a través del artículo 1[23] de la ley 1273 de 2009.

Otro instrumento normativo que podremos citar como ejemplo, ya aquí de trascendencia internacional y probablemente el instrumento jurídico internacional más importante en materia de delitos informáticos, es el Convenio de Cibercrimen de Budapest[24]. Sin entrar en mayores detalles que serían necesarios para explicar dicho convenio, diremos brevemente que en el Capítulo II, sobre medidas que deben adoptarse a nivel nacional, en la Sección 1 - Derecho penal sustantivo, el Título 1 se denomina "*Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos*".

Continuando con el tema del bien jurídico, nos parece apropiado abordar aquí una de las características de los delitos informáticos: su carácter de pluriofensivos. Es decir, son delitos en los cuales es posible encontrar la afectación de más de un bien jurídico a la vez.

En el caso de los delitos informáticos, una estafa electrónica puede afectar la confidencialidad de la información, su integridad y el patrimonio (en función del sistema atacado) y puede abarcar también delitos que ataquen el orden económico y financiero.

Para los autores chilenos Claudio Magliona y Macarena López[25], los delitos informáticos tienen el carácter de pluriofensivos o complejos, es decir "*que se caracterizan porque simultáneamente protegen varios intereses jurídicos, sin perjuicio de que uno de tales bienes está independientemente tutelado por otro tipo*".

En palabras de estos autores, el nacimiento de esta nueva tecnología está proporcionando "*nuevos elementos para atentar contra bienes ya existentes (intimidad, seguridad*

(21) Modificación realizada por la L. 26388

(22) Acurio del Pino, Santiago: "Generalidades de los delitos informáticos" - Ver en: oas.org

(23) Art. 1 - "Adiciónase el Código Penal con un Título VII BIS denominado 'De la Protección de la información y de los datos', del siguiente tenor: Capitulo. I - 'De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos'"

(24) Council of Europe: "Convenio de Cibercriminalidad de Budapest" - Budapest - 23/11/2001. Ver en: coe.int - Consultado el 10/4/2017

(25) Magliona Markovicth, Claudio P. y López Medel, Macarena: "Delincuencia y fraude informático" - Ed. Jurídica de Chile - 1999

nacional, patrimonio, etc.), sin embargo han ido adquiriendo importancia nuevos bienes, como sería la calidad, pureza e idoneidad de la información en cuanto tal y de los productos de que ella se obtengan; la confianza en los sistemas informáticos; nuevos aspectos de la propiedad en cuanto recaiga sobre la información personal registrada o sobre la información nominativa".

A modo de cierre de esta sección, afirmamos que la inexistencia de consenso sobre el bien jurídico protegido en los delitos informáticos termina por derivar en problemas de aplicación final de los tipos penales. En nuestra opinión, consideramos que debe ser la información un nuevo bien jurídico protegido, como un bien intangible pero de claro valor en nuestra "sociedad de la información". Sin embargo, debemos puntualizar qué tipo de información deberemos proteger. ¿Es cualquier tipo de información susceptible de recibir el resguardo del arma más dura que tiene el derecho, el sistema penal? Opinamos que no, que no cualquier información debería ser protegida, o para ser más preciso, no cualquier aspecto de la información debería ser protegido.

Entendemos que los aspectos que deben ser considerados de valor jurídico son la confidencialidad, la integridad y la disponibilidad de la información, es decir, los tres pilares de la seguridad de la información desarrollados anteriormente. Desde esta óptica, será posible entender, por ejemplo, que en el caso de acceso indebido a un sistema informático, el bien jurídico afectado será la confidencialidad de la información. En el caso de daño informático (sabotaje para algunos autores), se afecta la integridad de la información. En el caso de la denegación de servicios, el bien jurídico afectado será la disponibilidad de la información. Los ejemplos dados son con fines didácticos, ya que, como se ha visto, muchos de estos delitos son pluriofensivos, por lo que, en el caso concreto, más allá de la afectación de estos valores de la información, además podrían ser afectados otros tantos -intimidad de una persona, patrimonio, entre otros-.

VII - CARACTERES DE LOS DELITOS INFORMÁTICOS

Antes de pasar a un desarrollo más pormenorizado de distintos desafíos que plantean los delitos informáticos, parece atinado citar a otro maestro del derecho informático y autor de una de las primeras obras relacionadas con el tema en nuestro país, el Dr. Horacio Fernández Delpech[26], quien en la última actualización de su obra detalla una serie de circunstancias que hacen que este tipo de ilícitos penales sean de difícil represión:

- *La falta de una tipificación específica en la mayoría de las legislaciones de los delitos informáticos y cometidos a través de la red;*
- *La transnacionalidad de las conductas, que muchas veces se realizan en un país, pero cuyos resultados se producen en otro;*
- *La falta de consenso internacional sobre la reprochabilidad de ciertas conductas;*
- *Las permanentes innovaciones tecnológicas, que generalmente avanzan más rápido que las implementaciones de soluciones normativas;*

Como se observa, el Dr. Fernández Delpech nos trae una primera serie de características propias de los delitos aquí en estudio, entre las que podemos encontrar la

(26) Fernández Delpech, Horacio: "Manual de derecho informático" - 1ª ed. - Ed. AbeledoPerrot – Bs. As. - 2014 - pág. 194

transnacionalidad, la falta de legislación adecuada y la falta de coordinación penal entre los países, aspectos que a continuación desarrollaremos.

En palabras de Pablo Palazzi, uno de los autores más reconocidos en la materia penal informática, "*cabe resaltar la magnitud de los daños, la cada vez más frecuente naturaleza global e internacional de esta clase de delitos; la facilidad para cometerlos; y las dificultades para la investigación, que ha llevado a la necesidad cada vez mayor de cooperación entre fuerzas de seguridad y el sector privado por la necesidad de preservar datos en el tráfico de ISP, servidores y finalmente, las empresas de hosting y numerosas reconfiguraciones de los esquemas tradicionales con los cuales se concibe el derecho penal*".[27]

Otro autor que se anima a indicar características propias es el Dr. Julio Téllez Valdés[28], para quien los delitos informáticos presentan las siguientes características principales:

1. *Son conductas criminales de cuello blanco* (white collar crime)*, en tanto que solo un determinado número de personas con ciertos conocimientos (en este caso técnicos) puede llegar a cometerlas.*
2. *Son acciones ocupacionales, en cuanto a que muchas veces se realizan cuando el sujeto se halla trabajando.*
3. *Son acciones de oportunidad, ya que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico.*
4. *Provocan serias pérdidas económicas, ya que casi siempre producen "beneficios" de más de cinco cifras a aquellos que las realizan.*
5. *Ofrecen posibilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a consumarse.*
6. *Son muchos los casos y pocas las denuncias, y todo ello debido a la misma falta de regulación por parte del Derecho.*
7. *Son muy sofisticados y relativamente frecuentes en el ámbito militar.*
8. *Presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico.*
9. *Tienden a proliferar cada vez más, por lo que requieren una urgente regulación. Por el momento siguen siendo ilícitos impunes de manera manifiesta ante la ley.*

Abordaremos el estudio de varias de las características citadas por estos autores, más otras que considero que deben destacarse.

1. Delitos de cuello blanco

Tradicionalmente se ha considerado que los delitos informáticos son de cuello blanco (*white collar crimes*) ya que solamente podían ser realizados por un limitado grupo de personas con conocimientos avanzados y, en algunos casos, profesionales. En la actualidad considero que es una categoría que no parece ser tan exacta para este tipo de delitos, toda vez que la evolución en materia de (in)seguridad informática ha llevado a que los conocimientos sean cada vez más accesibles y difundidos. Además, las posibilidades

(27) Palazzi, Pablo A.: "Delitos informáticos" - Ed. Ad-Hoc - Bs. As. - 2000

(28) Téllez Valdés, Julio: "Derecho informático" - 3ª ed. - Ed. Mc Graw Hill - México - 2003 - pág. 8

de acceder a *rootkits*[29] -incluso de forma gratuita y al alcance de un par de clics- terminan generando toda una nueva generación de ciberdelincuentes que ya no poseen grandes conocimientos sobre el funcionamiento de un sistema, sino que son meros ejecutores de herramientas realizadas por terceros.

Esta apreciación tiene mucho que ver con el desarrollo que ha tenido la ciberdelincuencia en los últimos años, sobre todo aquellas bandas organizadas (cibercrimen) y especializadas en este tipo de delitos. Es decir, el cibercrimen como negocio demanda un aumento en la cantidad de ataques para que sea redituable. Son realizados de forma masiva en todas partes del mundo (transnacionalidad del delito), y por lo tanto, la automatización de los ataques alienta la generación de herramientas que realizan todas las tareas de forma automatizada. Por lo tanto, existe una gran cantidad de ciberdelincuentes que realizan estas tareas, pero que realmente no comprenden todo el conocimiento que hay en la construcción de la misma, ni saben cuál es la vulnerabilidad explotada ni la forma en que se explota o se escalan los privilegios.

En conclusión, considero que esta característica ya ha quedado atrasada en el tiempo; a diferencia de los ciberdelincuentes de la vieja escuela, a las nuevas generaciones poco les interesa el conocimiento, sino que están interesados en los "beneficios".

De hecho, de esta última apreciación se desprende una de las grandes diferencias entre los verdaderos *hackers* y los *crackers*, tópico sobre el cual realizaré algunas apreciaciones hacia el final del capítulo, ya que su significado es relevante para todo aquel lector que quiera acercarse y comprender realmente el funcionamiento del mundo de la ciberdelincuencia.

2. Transnacionales

La posibilidad tecnológica de las comunicaciones a distancia a través de las redes conciben que el delincuente se encuentre físicamente alejado (incluso por medio de varios países) de la víctima. Esta característica es de relevancia ya que, en el caso del cibercrimen, las bandas organizadas suelen realizar los delitos desde determinados países (por ej., India, Moldovia, Rumania, etc.) cuyas características propias -complicaciones de idioma, falta de legislación en la materia, falta de cooperación internacional para la justicia, entre otros- hacen que las investigaciones sean de alto nivel de complejidad, con un nivel de eficacia prácticamente nulo.

La internacionalidad, como propiedad de los delitos informáticos, implica que los mismos no encuentran barreras jurisdiccionales para llevarse a cabo. Es decir, técnicamente es posible estar conectado a una red en Argentina, pasar por un *router*[30] conectado en Rusia, utilizar una *botnet*[31] de computadoras en Colombia y finalmente atacar un sistema en Cuba. Por más complejo que pueda parecer en los papeles, a nivel práctico es de relativa facilidad, siempre que se cuente con un mínimo de conocimientos técnicos.

(29) El término proviene de una concatenación de la palabra inglesa *root*, que significa "raíz" (nombre tradicional de la cuenta privilegiada en los sistemas operativos Unix) y de la palabra inglesa *kit*, que significa "conjunto de herramientas" (en referencia a los componentes de *software* que implementan este programa)

(30) Un *router* o enrutador es un dispositivo que proporciona conectividad a nivel de red

(31) Una *botnet* es una red de computadoras "zombies", es decir que han sido previamente infectadas y que permiten que quien tenga su control pueda utilizarlas como armas para distintos tipos de ataques

Estos casos vuelven a poner sobre las mesas de los académicos las clásicas preguntas sobre la legislación aplicable, pero sobre todo postula el claro desafío de coordinar distintos ámbitos de colaboración internacional. En relación con este último aspecto, el Convenio de Cibercriminalidad de Budapest(32), del que ya hemos hablado anteriormente, es el instrumento internacional más importante en la materia precisamente porque apunta a tener dentro de los Estados firmantes un mínimo de coordinación en el ámbito penal material, y un potente marco de cooperación internacional (procesal penal) para la investigación de estos casos.

Argentina es un flamante nuevo miembro de este Convenio, que a través de la ley 27411 ratificó su adhesión, aunque con algunas reservas(33): nuestro país tiene tareas pendientes en distintos aspectos que debe cumplimentar para formar parte de dicho grupo, especialmente en materia procesal penal.

Más allá de la necesidad de cooperación internacional, consideramos importante marcar la necesidad de un previo marco de cooperación nacional en Argentina. En la actualidad se pueden observar diferentes realidades en nuestro país, que dependen del grado de desarrollo o fortaleza económica de cada Provincia en particular. A modo de ejemplo, podría mencionarse que las víctimas de la Ciudad Autónoma de Buenos Aires poseen la posibilidad de denuncia ante la División de Delitos Tecnológicos de la Policía Federal Argentina o ante el Área Especial de Investigaciones de Telemáticos de la Policía Metropolitana de la Ciudad Autónoma de Buenos Aires, opciones que no existen en la mayoría de las otras Provincias de nuestro país.

Dada la heterogeneidad de situaciones hacia el interior de nuestro país, se propone considerar la necesidad de generar una "*Red Nacional de Cooperación en materia de Delitos Informáticos*", para que aquellas Provincias (Catamarca, Jujuy, Entre Ríos, Santa Fe, etc.) que aún no tienen una estructura armada en la materia puedan acceder a los avances y experiencias de otras con mayor desarrollo en el área (tales como Bs. As. cdad. y Córdoba), así como poseer canales ágiles de cooperación para los casos que requieran colaboración interjurisdiccional.

3. Instantáneos

Esta característica tiene más bien que ver con algo propio de las nuevas tecnologías (al igual que la comisión a distancia), toda vez que el momento de realización es instantáneo, más allá del eventual tiempo que podría llevar la inteligencia preliminar o preparación de un ataque determinado. Es decir, el perfeccionamiento del delito se da en el mismo momento en que el delincuente lleva adelante la acción. Pensemos, como ejemplo, casos de accesos indebidos a sistemas o datos restringidos -*hacking*-, daños informáticos -*cracking*-, o la denegación de servicio de un sitio web por unas horas.

4. Masivos

Esta característica en la comisión de los delitos informáticos tiene relación directa con las posibilidades tecnológicas de difusión masiva de contenidos, con interdependencia de la instantaneidad antes analizada. A modo de ejemplo, podríamos mencionar los casos de *spam con ataques de phishing* masivo o casos de envío masivo de correos electrónicos

(32) Council of Europe: "Convenio de Cibercriminalidad de Budapest" - Budapest - 23/11/2001. Ver en: coe.int – Consultado el 27/6/2017

(33) Segu-Info - Ver en: blog.segu-info.com.ar

que esconden entre sus adjuntos *malware* listo para infectar los equipos de las víctimas -*ransomware*-. Por otro lado, el aumento de la generación de herramientas que automatizan el proceso de detección de sistemas vulnerables, junto con su explotación e infección posterior, permite que los delincuentes activen recursos que realizan ataques masivos alrededor del mundo, buscando víctimas que no han tomado los recaudos de seguridad de la información necesarios -como por ejemplo la actualización de sus sistemas operativos, como ocurrió en el caso de Wannacry-.[34]

5. Anonimato

Con esta característica nos referimos a la posibilidad de lograr distintos niveles de anonimato que presentan las nuevas tecnologías. Es decir que la persona que las utiliza pueda ocultar su verdadera identidad, o en el caso de las redes, la verdadera conexión desde la cual está llevando adelante sus acciones.

El primer comentario que debemos tener en cuenta es que el anonimato no debe ser tomado en sí como solamente negativo, toda vez que esta característica como tal permite que muchas personas que se encuentran en contexto de persecución o censura puedan ver efectivizados sus derechos de libre acceso a la información y libre expresión en las redes, gracias a estas tecnologías que permiten evitar su verdadera identificación.

Como hemos sostenido al iniciar este trabajo, las tecnologías son neutras y su valoración dependerá pura y exclusivamente de lo que el hombre en sí decida hacer con ellas. En el caso de la comisión de delitos informáticos, las distintas técnicas de anonimato existentes -en el caso que sean utilizadas- llevan al investigador a enfrentarse con un complejo desafío al momento de intentar determinar al autor de un delito.

Sin embargo, debemos hacer notar que, así como es posible afirmar que ninguna tecnología es 100% segura, también es posible afirmar que ninguna tecnología ofrece un 100% de anonimicidad para el usuario. Por eso consideramos más adecuado, desde una óptica técnica-jurídica, hablar de niveles de anonimato que, dependiendo del tipo de tecnología, implicarán un desafío mayor o menor para el investigador. A modo de ejemplo breve, no es el mismo nivel de anonimato el de un delito cometido desde un wifi público (un nivel bajo de anonimato) que el de un delito cometido desde la red TOR -una de las puertas de entrada para la *Deep web*-, en el cual existe un encadenamiento de *proxy*s anónimos que complejiza mucho más la investigación.

Desde la seguridad de la información, siempre hemos tenido precauciones al hablar o escribir sobre la *Deep web*, básicamente porque mucha de la información ahí disponible no está verificada ni puede ser adecuadamente comprobada, al menos no con la rigurosidad académica que es necesaria para este tipo de trabajos. En Internet se puede encontrar una importante cantidad de artículos[35] publicados en diversos medios, algunos incluso diarios de importantes nombres[36], donde se brindan estadísticas sobre la cantidad de contenidos y se afirman determinados datos que no poseen ningún tipo de fuente, o, si las supuestas fuentes existen, la información no se encuentra adecuadamente fundada.

(34) "Wannacry: al menos 75 países afectados" - Segu-Info - Ver en: blog.segu-info.com.ar

(35) Telam: "La internet profunda, adonde navega el delito" - Ver en: telam.com.ar – Consultado el 12/6/2017

(36) "Sicarios, drogas y pornografía infantil, los delitos que esconde la Dark Web" - Diario Clarín - Ver en: clarin.com. Consultado el 12/6/2017

No obstante, diremos que la *Deep web* es un espacio virtual más que existe en la actualidad, cada vez más accesible para los usuarios, y que posee determinadas características que es necesario considerar si se quiere hacer un estudio completo sobre los delitos informáticos[37]. Esta *Deep web* (también llamada Internet profunda o Internet oculta) no es más que una parte de la red de Internet en la cual los contenidos no son indexados por los motores de búsquedas tradicionales (Google, Yahoo, Bing, etc.). Por ello, y en contraste con la *Deep web*, a Internet como lo conocemos se lo conoce también como "Internet superficial".

Los contenidos pueden no ser indexados por distintas razonas, entre las que encontraremos: páginas web dinámicas, sitios bloqueados (por un CAPTCHA, por ejemplo), sitios privados (acceso solo con "logueo" previo), sitios con contenidos que no son HTML, así como redes de acceso limitado (por ejemplo, a determinados protocolos de accesos). Dentro de estos últimos, de contenidos que solo son accesibles a través de un determinado *software* o protocolo específico, podemos encontrar al Proyecto TOR[38], una de las herramientas más conocidas, que construye un circuito de conexiones cifradas a través de repetidores en la red, donde el circuito se extiende un salto a la vez. Cada nodo a lo largo del camino conoce únicamente el nodo que le proporciona los datos y retransmite los que les entrega. De esta forma un nodo, de forma individual, nunca conoce el recorrido completo que ha tomado un paquete de datos. El cliente negocia un paquete separado de claves de cifrado para cada tramo a lo largo del circuito, asegurando que la información circulante entre los nodos no pueda ser rastreada.

El circuito de conexión a través de tres nodos distintos cambia aproximadamente cada diez minutos -depende de la configuración del usuario-, dificultando aún más cualquier intento de análisis o *tracking* de las conexiones circulantes por los nodos.

Todo este esfuerzo tecnológico fue premiado en marzo de 2011 cuando TOR recibió, de la *Free Software Foundation,* un premio para proyectos de beneficio social por "*haber permitido que, aproximadamente, 36 millones de personas de todo el mundo, usando software libre, hayan experimentado libertad de acceso y de expresión en Internet manteniendo su privacidad y anonimato. Su red ha resultado crucial en los movimientos disidentes de Irán y Egipto*".[39]

(37) Temperini, Marcelo: "*Deep web*, anonimato y cibercrimen" - VI Congreso Iberoamericano de Investigadores y docentes de derecho e informática (CIIDDI 2016) - ISBN: 9789876921381 - 2016

(38) Creado en 2003 por Roger Dingledine, Nick Mathewson y Paul Syverson, surgió como la evolución del proyecto Onion Routing del Laboratorio de Investigación Naval de los Estados Unidos. A finales de 2004 pasó a ser patrocinado por la Electronic Frontier Foundation, la organización de defensa de libertades civiles en el mundo digital, hasta noviembre de 2005. Actualmente el proyecto Tor está en manos del 'Tor project' una organización sin ánimo de lucro orientada a la investigación y la educación, radicada en Massachusetts y que ha sido financiada por distintas organizaciones. Es un proyecto cuyo objetivo principal es el desarrollo de una red de comunicaciones distribuida de baja latencia y superpuesta sobre Internet, en la que el encaminamiento de los mensajes intercambiados entre los usuarios no revela la identidad de la conexión (dirección IP), permitiendo un anonimato a nivel de red y que, además, mantiene la integridad y el secreto de la información que viaja por ella. Para la consecución de estos objetivos se ha desarrollado un software libre específico, que propone el uso de una ruta de conexión del tipo "cebolla", es decir donde los mensajes viajen desde el origen al destino saltando a través de distintos routers ubicados en distintos puntos del mundo, generando un sistema de protección de la identidad de varias capas (de allí sale el nombre de cebolla). Más información en torproject.org

(39) CENATIC: "Premian a Tor Project por su protección del anonimato en la red" - Ver en: cenatic.es - Consultado el 12/6/2017

6. Pluriofensivos

Hemos ya señalado que estamos ante delitos en los cuales es posible encontrar la afectación de más de un bien jurídico a la vez. En el caso de los delitos informáticos, y a modo didáctico, citaremos un caso reciente sobre un ataque informático contra el sitio web del Ejército Argentino(40), en el que se inscribieron consignas vinculadas al grupo terrorista ISIS(41). En principio, y por la información disponible, se trata de un *deface*(42) de un sitio web, que desde un punto de vista jurídico puede ser considerado como un caso de daño informático (art. 183, segundo párr. del Código Penal). El bien jurídico afectado sería la confidencialidad y la integridad de la información (que no solo fue accedida ilegítimamente, sino que además fue alterada). A su vez, podríamos considerar que podría existir -en el caso citado de la web del Ejército Argentino-, un delito que además compromete la paz y la dignidad de la Nación.(43)

A modo de observación, aprovechamos la ocasión para expresar nuestra disidencia con algunos autores, que suelen vincular los daños de los delitos informáticos exclusivamente a grandes pérdidas económicas. En primer lugar, no consideramos correcto relacionar exclusivamente los delitos informáticos con los daños directamente económicos, toda vez que muchos de ellos afectan la intimidad, privacidad, honor, reputación, e incluso hasta la integridad o normal desarrollo sexual de los menores -casos de *grooming*-. Entendemos que muchos de los grandes informes sobre cibercrimen a nivel mundial (Symantec, Panda, TrendMicro, entre otros) tienden a realizar estas asociaciones económicas sobre el cibecrimen, ya que buscan generar en el lector de los informes -potenciales clientes de los servicios de prevención en materia de seguridad informática que esas mismas empresas ofrecen- una sensación de inseguridad y de justificación de la inversión que deberían realizar para mejorar los niveles de seguridad de sus sistemas de información.

En segundo lugar, también nos permitimos dudar de la afirmación de que los beneficios para los delincuentes siempre sean enormes, toda vez que incluso en aquellos delitos informáticos cuyo objetivo directo es la afectación del patrimonio de la víctima (como las estafas electrónicas), salvo excepciones, por lo general suelen ser de poco monto (conocido de modalidad hormiga) con el fin de que la víctima no se dé cuenta y el fraude se mantenga la mayor cantidad de tiempo posible.

Por otro lado, en los casos conocidos (y citados en estos grandes informes) como "robo de información"(44), la valoración económica sobre las pérdidas es totalmente subjetiva, ya que todo dependerá del tipo de información de que se trate.

(40) "Hackean con una leyenda de la web del Ejército" - Diario La Nación - Ver en: lanacion.com.ar - Consultado el 20/6/2017

(41) En el sitio web del Ejército podía leerse "Somos el Estado Islámico Allahu Akbar. - Esto es una amenaza. ISIS está en Argentina y muy pronto van a saber de nosotros. Allahu Akbar"

(42) El *defacing* es la práctica de, sin consentimiento de sus legítimos titulares, modificar o alterar la portada de un sitio web. Los motivos de esta práctica (muy común en el ámbito de la seguridad informática), suelen ser cuestiones ideológicas (buscan dar un mensaje), políticas, religiosas, y, en algunos casos, simplemente por diversión de los atacantes, para quienes la captura de pantalla del deface sirve en muchos casos como una "medalla" que tiene cierto valor en un sistema de meritocracia

(43) Tít. IX: Delitos contra la seguridad de la Nacion; Cap. II: Delitos que comprometen la paz y la dignidad de la Nación, Código Penal de la Nacion Argentina; L. 11179

(44) Si bien así se conoce popularmente a los casos de "fuga de información", disentimos en la denominación técnica de "robo de información" toda vez que consideramos que la información en sí no podría ser robada en los términos jurídicos penales

7. Investigación compleja

La combinación de varios de los aspectos de las nuevas tecnologías ya desarrollados hasta el momento tienen como consecuencia generar una investigación penal mucho más compleja que las tradicionales. Implica que las fuerzas de seguridad a cargo de dichas tareas tengan un mínimo de conocimientos técnicos, suficientes para comprender las maniobras delictivas y poder llevar adelante una investigación eficaz.

La investigación de los delitos informáticos estará marcada por la volatilidad de la evidencia digital, por lo que las fuerzas de seguridad deberán estar adecuadamente capacitadas para lograr una identificación, recolección y preservación de los datos, que deberá hacerse de acuerdo a las buenas prácticas internacionales(45) -y en algunos casos, a protocolos o guías nacionales-(46), garantizándose la cadena de custodia de todos los elementos que vayan a ser incorporados a la causa como prueba.

La cadena de custodia puede ser definida como el "*registro cronológico y minucioso de la manipulación adecuada de los elementos, rastros e indicios hallados en el lugar del hecho, durante todo el proceso judicial*"(47). Otro concepto más completo de autores nacionales(48) afirma que la cadena de custodia es una secuencia o serie de recaudos destinados a asegurar el origen, identidad e integridad de la evidencia, evitando que esta se pierda, destruya o altere. Se aplica a todo acto de aseguramiento, identificación, obtención, traslado, almacenamiento, entrega, recepción, exhibición y análisis de la evidencia, preservando su fuerza probatoria. Además, hace transparente todo eventual cambio o alteración del material probatorio. En otras palabras, si el proceso de la cadena de custodia no ha presentado alteraciones ni variaciones de ningún tipo durante su traslado y análisis, se dice que permite garantizar la autenticidad de la evidencia que se utilizará como prueba dentro del proceso judicial.

En relación con la necesidad de capacitación, en las conclusiones del último Congreso Internacional de derecho penal(49) -dedicado a la sociedad de la información y el derecho penal-, organizado por la Asociación Internacional de derecho penal, se afirmó que "*los Estados han de asumir la obligación de proveer a las fuerzas policiales de los medios técnicos, las capacidades y la formación especializada en el uso de las TIC, no solo para luchar de manera eficaz contra las formas sofisticadas de cibercrimen, sino también para obtener y manejar correctamente la prueba electrónica en general. Se promoverá el desarrollo de guías de buenas prácticas en el uso de las TIC con fines de investigación criminal*". En las mismas resoluciones se reconoce que las medidas de investigación que impliquen el uso de las TIC y que representen una intromisión significativa en el derecho a la privacidad (como el acceso al contenido de las comunicaciones, la interceptación y el acceso de datos en tiempo real, o la utilización de técnicas de investigación remota) solo

(45) Una de las normas más importantes al respecto es la norma internacional ISO/IEC 27037:2012 "Information technology - Security techniques - Guidelines for identification, collection, acquisition and preservation of digital evidence"

(46) Procuración General de la Suprema Corte de Justicia de la Provincia de Buenos Aires. Protocolo de Cadena de Custodia. R. 889/2015 - Ver en: mpba.gov.ar - Accesible: julio 2016

(47) Torales, Eloy E.: "Manual de procedimiento para la preservación del lugar del hecho y la escena del crimen" - Ed. Ministerio de Justicia y Derechos Humanos de la Nación - Ver en: saij.gob.ar

(48) Di Iorio, Ana H.: "El rastro digital del delito: aspectos técnicos, legales y estratégicos de la informática forense" - 1ª ed. - Universidad FASTA - Mar del Plata - 2017

(49) XIX Congreso Internacional de Derecho Penal, Asociación Internacional de Derecho Penal - Río de Janeiro, 31 agosto - 6/9/2014. Tema: "Sociedad de la información y derecho penal"

podrán acordarse, como regla general, previa autorización judicial, cuando exista una sospecha razonable de la comisión de un delito que pueda calificarse como grave y de que el destinatario de la medida está vinculado con ese hecho delictivo.

Otro desafío sobre la investigación de este tipo de delitos consiste en la necesidad de cooperación de empresas privadas y proveedores de tecnología de información y comunicaciones (TIC) con las autoridades policiales en la investigación criminal. En relación con este tema debemos afirmar que hasta el momento de la redacción de estas líneas no existe en Argentina una normativa que obligue a los proveedores de servicios de internet (ISP) a guardar las direcciones IP asignadas a sus clientes por algún plazo determinado. En consecuencia, es posible que al realizar una investigación penal sobre algún hecho (y teniendo identificada la dirección IP del autor del delito) aun contando con la autorización judicial correspondiente no se pueda lograr identificar a la persona que la tenía asignada en un momento determinado, toda vez que algunas empresas no guardan dicha información o en el caso de guardarlas deciden no colaborar con la justicia.

VIII - CONCLUSIONES

A modo de reflexión final sobre lo trabajado, se puede concluir que la situación en Argentina en relación con la lucha contra los delitos informáticos y el cibercrimen presenta variados y diversos desafíos.

Si bien la idea del presente trabajo ha sido introducir al lector a una serie de consideraciones preliminares sobre el estudio de los delitos informáticos, a pocos metros de nuestra largada hemos encontrado e intentado desarrollar distintos aspectos y características propias que, al menos desde nuestra óptica, son necesarios para abordar un tema tan complejo.

Entendemos que debemos comprender que la sanción de la llamada ley 26388 de delitos informáticos de Argentina debe ser considerado como un puntapié inicial en este camino, y no como un final en sí mismo.

Si bien es necesario contar con una normativa adecuada, por sí sola la norma no es suficiente. Es decir, la tipificación de una conducta disvaliosa como delito no es más que un reconocimiento jurídico, pero la norma por sí sola no combate en la práctica todos aquellos delitos que ocurren y que, en la mayoría de los casos, no forman parte de ninguna estadística, pasando a formar parte de la cifra negra.

La superación o mitigación de estos desafíos que nos presentan los delitos informáticos involucran aspectos técnicos, jurídicos, socioculturales y políticos que requieren mejorar los niveles de capacitación de todos los actores intervinientes en el proceso judicial, así como un abordaje serio por parte del Estado (en sus distintos niveles), basado en la previa comprensión y dimensionamiento de la problemática que implica el cibercrimen en Argentina.

TENENCIA SIMPLE DE PORNOGRAFÍA INFANTIL Y FIGURAS CONEXAS

Marcelo A. Riquert(*)

I - INTRODUCCIÓN

La del artículo 128 del Código Penal es una de las tantas tipicidades que han sido objeto de recientes y sucesivas reformas en su texto. Uno de los factores que incidieron para la introducción de estos cambios fue, sin duda, la incidencia del factor tecnológico para su comisión(1) y, por eso, dentro de lo que fue una masiva actualización de figuras penales bajo tal consideración, fue sustituido por el artículo 2 de la ley 26388(2). Pese a que el espíritu general de dicha ley fue abrir el camino hacia la suscripción del Convenio sobre Ciberdelito de Budapest (2001; en vigor desde el 1/7/2004), en materia de las propuestas de tipificación de tenencia de pornografía infantil se ciñó a incorporar aquella que fuera con fines inequívocos de distribución o comercialización (segundo párrafo, ahora desplazado a tercero en el texto vigente).

(*) Abogado y doctor en Derecho (UNMDP). Máster en Derecho Penal (Universidad de Salamanca, España). Profesor titular ordinario y director del Departamento de Derecho Penal y Criminología y de la carrera de posgrado de Especialización en Derecho Penal (UNMDP)

(1) Fernando Miró Llinares, quien resalta que *"el fenómeno de la pornografía infantil, a pesar de no ser propiamente informático, está cada vez más vinculado al uso de las nuevas tecnologías de la información, hasta tal punto que, en la actualidad, desde una perspectiva criminológica puede decirse que la mayoría de estos comportamientos se perpetran básicamente a través de Internet"* (en su obra "El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio" - Ed. Marcial Pons - Madrid - 2012 - pág. 107). Gustavo E. Aboso, quien sostiene que, sin temor a equívoco, este género delictivo fue el que más se aprovechó de la utilización abusiva de la red informática, circunstancia que halló eco en los gobiernos en general, preocupados en poner coto a un auténtico flagelo que tiene por víctimas a los menores de edad y que afecta gravemente su indemnidad sexual, dejando huellas profundas e indelebles en sus inocentes psiquis (en su obra "Derecho penal cibernético" - Ed. BdeF - Montevideo/Bs. As. - 2017 - pág. 202)

(2) BO: 25/6/2008

Es más, tras un largo proceso, al momento de aprobarse dicho Convenio mediante la ley 27411[3], se había formulado reserva con relación a la denominada "tenencia simple", señalando en el inciso c) de su artículo 2: *"La **República Argentina** hace reserva parcial del artículo 9.1.e. del **Convenio sobre Ciberdelito** y manifiesta que no regirá en su jurisdicción por entender que el mismo solo es aplicable de acuerdo con legislación penal vigente hasta la fecha, cuando la posesión allí referida fuera cometida con inequívocos fines de distribución o comercialización (artículo 128, segundo párrafo, del **Código Penal**)".*

El mismo legislador, apenas tres meses después, decide incorporar como nuevo segundo párrafo al Código Penal justamente la propuesta de conducta típica respecto de la que se había realizado reserva. Lo hizo por el artículo 1 de la ley 27436[4], que incorporó el actual segundo párrafo. En definitiva, la redacción vigente es la siguiente:

> *"**Artículo 128** - Será reprimido con prisión de seis (6) meses a cuatro (4) años el que produjere, financiare, ofreciere, comerciare, publicare, facilitare, divulgare o distribuyere, por cualquier medio, toda representación de un menor de dieciocho (18) años dedicado a actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales, al igual que el que organizare espectáculos en vivo de representaciones sexuales explícitas en que participaren dichos menores.*
>
> *Será reprimido con prisión de cuatro (4) meses a un (1) año el que a sabiendas tuviere en su poder representaciones de las descriptas en el párrafo anterior.*
>
> *Será reprimido con prisión de cuatro (4) meses a dos (2) años el que tuviere en su poder representaciones de las descriptas en el párrafo anterior con fines inequívocos de distribución o comercialización.*
>
> *Será reprimido con prisión de un (1) mes a tres (3) años el que facilitare el acceso a espectáculos pornográficos o suministrare material pornográfico a menores de catorce (14) años".*

En lo que sigue, se hará un comentario tanto de la nueva, precedida -por cierto- de contrapuestas opiniones[5], como de las precedentes tipicidades.

(3) BO: 15/12/2017

(4) BO: 23/4/2018

(5) La ardua discusión entre quienes argumentaron a favor y en contra de la tipificación de la simple tenencia es presentada con detalle por Dupuy, Daniela en su trabajo "La posesión de pornografía infantil", en AA. VV.: "Cibercrimen", bajo su propia dirección - Ed. BdeF - Montevideo/Bs. As. - 2017 - pág. 123 y ss. Aclara la nombrada que su postura personal, favorable, se apoya en la realidad empírica de su práctica en el ámbito de la Fiscalía Especializada en Delitos Informáticos de la Ciudad de Buenos Aires (en particular, págs. 140/3)

II - CONSIDERACIONES EN TORNO AL BIEN JURÍDICO

Lo relativo a la genealogía del tipo, así como la legislación regional comparada, puede consultarse en trabajos previos a los que remito[6]. En lo inmediato, corresponde limitarse a recordar que la norma en comentario se inserta dentro del Título III "Delitos contra la integridad sexual", rúbrica conforme ley 25087[7], que reemplazó la original de "Delitos contra la honestidad".

Luego de la reforma, siguiendo en este punto a Cafferata Nores, parece claro que *"el objetivo primario de la incriminación reside en reprimir la explotación de niños en la producción de imágenes pornográficas"*[8]. De lo expuesto se puede colegir que ya no se protege lo que puedan ver mayores de edad, sino que el paradigma es otro: es la prohibición de utilizar menores de 18 años para la realización de las acciones que describe la norma, en cuanto implican un ataque a la indemnidad o integridad sexual de los menores, sin diferencia obviamente de sexo, ni interferencias de terceros en su desarrollo.

Por eso, tanto Gavier[9] como Reinaldi[10] apuntan que el bien jurídico que se ha querido tutelar es el normal desarrollo psíquico y sexual de quienes no han cumplido la edad de dieciocho años y que, por lo tanto, no han alcanzado suficiente madurez, e impedir que se recurra a ellos para protagonizar esas representaciones sin medir los daños que a causa de ello puedan sufrir. Aboso apunta no albergar duda en torno a que el interés jurídicamente protegido es el normal desarrollo sexual de las personas menores de edad desde la perspectiva de no ser expuestas a la explotación sexual por parte de terceros[11], agregando que la tipificación de tenencias como las del actual tercer párrafo tienen como propósito central el desalentar cierto tipo de prácticas o actividades sexuales que involucran necesariamente a los adultos (así, la promoción o incitación a la pedofilia) o directamente las agresiones sexuales contra menores de edad. Se trataría de una forma de luchar contra el mercado de la pornografía infantil e incentivar contra la explotación sexual de los menores de edad.[12]

(6) Así, el comentario al art. 128, CP realizado en AA.VV.: "Código Penal y normas complementarias. Análisis doctrinal y jurisprudencial", Zaffaroni, Eugenio R. y Baigún, David (Dirs.) - 2ª ed. - Ed. Hammurabi - Bs. As. - 2010 - T. 4 - pág. 735 y ss. Asimismo, en el trabajo en coautoría con Riquert, Fabián L. titulado "Derechos humanos: La protección constitucional y penal de los niños frente a la pornografía infantil", pub. en la Revista Jurídica do Cesuca - Río Grande do Sul - Brasil - N° 4 - diciembre/2014 - vol. 2 - págs. 140/58 (disponible en http://ojs.cesuca.edu.br/index.php/revistajuridica)

(7) BO: 14/5/1999

(8) "Antecedentes Parlamentarios" - LL - N° 5 - junio/1999 - año VI - pág. 1616

(9) Gavier, Enrique A.: "Delitos contra la integridad sexual. Análisis de la ley 25087" - Marcos Lerner Editora - Córdoba - 1999 - pág. 89

(10) En su obra "Los delitos sexuales en el Código Penal argentino. Ley 25087" - Marcos Lerner Editora - Córdoba - 1999 - pág. 206

(11) Aboso, Gustavo E.: "Derecho penal cibernético" - Ed. BdeF - Montevideo/Bs. As. - 2017 - pág. 207

(12) Aboso, Gustavo E.: "Derecho penal cibernético" - Ed. BdeF - Montevideo/Bs. As. - 2017 - pág. 209

He agregado, en su oportunidad, patentizando la complejidad del objeto de protección, a la dignidad del menor que es ciertamente un bien jurídico comprendido y al que se atiende cuando se penalizan conductas como las de producción, publicación o distribución de imágenes pornográficas en las que se exhiben menores. A partir del perfeccionamiento de la edición de imágenes digitales (*morphing*) y en función de las modalidades de tipificación que reclaman, por un lado, el citado Ciberconvenio y, por otro, el Protocolo facultativo de la *Convención sobre los Derechos del Niño relativo a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía* -Asamblea General de Naciones Unidas, del 25/5/2000-, incorporado como ley 25763[13] [en cuanto su art. 2, inc. c), incluye dentro del concepto de pornografía infantil representaciones "reales o simuladas" de un niño dedicado a actividades sexuales explícitas], se podría decir que cuando se trata de supuestos de pornografía "técnica" o "virtual", es decir, aquella en la que un niño no ha sido efectivamente víctima partícipe en actos sexuales concretos sino que se altera o compone una imagen que lo incluye parcialmente sin que hubiera ninguna correspondencia real con un acto efectivo que dañe su normal desarrollo psicosexual, aparece como más evidente la nota de pluriofensividad y que, en este último supuesto, lo que se afecta es la dignidad del menor.

Parece participar de esta última idea la fiscal Daniela Dupuy, cuando apunta que quien posee pornografía infantil perpetúa un ataque a la dignidad de los niños que han sido previamente filmados y/o fotografiados. Además, puede contribuir al mantenimiento y expansión de futuras actividades criminales contra menores, para generar nuevo material con el fin de satisfacer la demanda.[14]

El límite de edad viene establecido por normas convencionales con jerarquía constitucional [art. 75, inc. 22), CN]. Así, la Convención sobre los Derechos del Niño que establece en el artículo 1 hasta los 18 años de edad para ser considerado menor y que, por ende, el legislador nacional no lo puede trasvasar [art. 75, inc. 12), CN]. Con acierto, advierte Reinaldi que debería ampliarse la protección comprendiendo no solo a los menores de edad, sino también a los incapaces, como lo hace el código penal español.[15]

El tráfico de material y producción de contenidos de pornografía vinculada a los menores genera alto nivel de consenso en cuanto a la necesidad de afrontarlo a nivel global. Es muy importante la cantidad de documentos suscriptos sobre el particular, partiendo de la Convención sobre los Derechos del Niño de Naciones Unidas, en vigor desde 1990, aprobada en la Argentina por ley 23849. Goza de jerarquía constitucional por vía del artículo 75, inciso 22), desde la reforma de la Carta Magna de 1994 y prevé en su artículo 34 la protección al menor *"contra todas las formas de explotación y abusos sexuales"*, formando parte de las obligaciones que impone, como resalta Marcelo P. Vázquez, *"la adopción de todas las medidas de carácter nacional, bilateral y multilateral 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; y la explotación del niño en espectáculos o materiales pornográficos"*.[16]

(13) BO: 25/8/2003

(14) Dupuy, Daniela: "La posesión de pornografía infantil", en AA.VV.: "Cibercrimen", bajo su propia dirección - Ed. BdeF - Montevideo/Bs. As. - 2017 - pág. 139

(15) En su obra "Los delitos sexuales en el Código Penal argentino. Ley 25087" - Marcos Lerner Editora - Córdoba - 1999 - págs. 206/7

(16) En su trabajo "La explotación sexual comercial de la niñez y su relación con la red Internet" - CDJP - Ad-Hoc - Nº 18-19 - Bs. As. - 2005 - pág. 646

III - ALGUNOS DATOS ESTADÍSTICOS

En nuestro país se carece tanto de trabajos de campo como estadísticos serios para cuantificar y cualificar la delincuencia informática. Recién entre 2017 y 2018 se ha dado a conocer por el Ministerio de Justicia y Derechos Humanos una serie de informes específicos -cuya confección estuvo bajo la dirección de Gustavo Sain- que proporcionan datos que corresponden a los años 2013 a 2016[17]. En lo que aquí interesa, revelan que tanto en el nivel federal como en la Provincia de Buenos Aires, los porcentuales de causas iniciadas para investigar algunos de los delitos introducidos por la mencionada reforma al Código Penal por ley 26388 son realmente ínfimos. Veamos algunos datos relevantes en los cuadros que siguen.

Cuadro 1[18]

(17) Se trata de una colección de "Estudios estadísticos sobre cibercrimen", constituida hasta ahora por los siguientes números: "Primer muestreo de denuncias judiciales de la República Argentina. Año 2013" (pub. en 2017); "Segundo muestreo de denuncias judiciales de la República Argentina. Año 2014" y "Tercer muestreo de denuncias judiciales de la República Argentina. Año 2015" (ambos pubs. en 2018). Por gentileza del director, he contado con un anticipo del "Cuarto muestreo de denuncias judiciales de la República Argentina. Año 2016". Todos los informes son publicados por Ediciones SAIJ - CABA. Hay versiones digitales disponibles en http://www.bibliotecadigital.gob.ar. El primer muestreo también está disponible como "Anexo I" en la obra de Sain, Gustavo y Azzolin, Horacio: "Delitos informáticos. Investigación criminal, marco legal y peritaje" - Ed. BdeF - Montevideo/Bs. As. - 2017 - págs. 89/139

(18) El cuadro presenta un segmento a la izquierda con datos nacionales y otro a la derecha con datos provinciales. A su vez, en su primera derivación, aporta las cifras totales y particulares en cada una de estas jurisdicciones, mientras que en la segunda derivación brinda datos de cantidad de causas por cada jurisdicción y proporción por población. Las siglas de los departamentos judiciales de Bs. As. corresponde a: LZ=Lomas de Zamora; MDP=Mar del Plata; LP=La Plata; BB=Bahía Blanca y SI=San Isidro

Puede advertirse que, en el fuero federal, no obstante el "salto" de ingresos generales (de 46043 a 84404), las investigaciones por casos de delincuencia informática bajaron de 221 a 119 entre 2013 y 2014. Aunque con aumento general menor y también disminución no tan intensa en lo específico, se observa la Provincia de Buenos Aires (en general incrementó de 694246 a 721501, en particular bajó de 275 a 245), en cuyo universo de casos los informáticos tienen un porcentual de una décima parte del federal por esos años.

Cuadro 2[19]

En el fuero federal, durante 2015, siguió en general una curva ascendente (97115) que no se sabe aún si se sostuvo en 2016. En lo particular, continuó bajando el número de causas por delincuencia informática: 112 en 2015 y solo 85 en 2016. En cambio, en la Provincia de Buenos Aires, al crecimiento suave de causas generales (719728 en 2015 y 746952 en 2016), lo acompaña una suba muy significativa en los casos por ley 26388, que pasan a ser 868 en 2015 y 1099 en 2016 (no obstante, en el porcentual general de 2015 recién ahora equiparan la baja proporción del fuero federal: 0,12%).

(19) Nuevamente, el cuadro presenta un segmento a la izquierda con datos nacionales y otro a la derecha con datos provinciales. A su vez, en su primera derivación aporta las cifras totales y particulares en cada una de estas jurisdicciones, mientras que en la segunda derivación brinda datos de cantidad de causas por cada jurisdicción y proporción por población. Las siglas de los departamentos judiciales de Bs. As. corresponde a: LZ=Lomas de Zamora; MDP=Mar del Plata; LP=La Plata; LM=La Matanza y SM=San Martín

Cuadro 3[20]

ARTÍCULO	DELITO	DENUNCIAS
197 183	Interrup o entorpecimiento de las comunicaciones Daño informático	'13 158 // 57 '14 4 // 2
153	Violación de correspondencia electrónica	26 // 30 1 // 8
255	Alteración de evidencia informática	16 // 11 127 // 87
157 157bis	Revelación de secretos Afectación datos personales	8 // 6 4 // 1
153bis	Acceso ilegítimo a sistema o dato informático	6 // 12 11 // 19
155 173	Pub. indebida de comunics Estafa informática	4 // 5 22 // 0
128	Distribución o comercio de pornografía infantil	3 // 1 106 // 128

Ahora se muestra el número de causas por delitos de la ley 26388 divididos por cada uno de los tipos correspondientes y la jurisdicción interviniente. Se advierte que los casos por el artículo 128 del Código Penal eran los segundos cuantitativamente en 2013 (109 entre ambas competencias juntas) y pasan a ser los más denunciados en 2014 (129 casos en conjunto).

Cuadro 4[21]

ARTÍCULO	DELITO	DENUNCIAS
197 183	Interrup o entorpecimiento de las comunicaciones Daño informático	'15 60+1/38+9 '16 11 // 11
153	Violación de correspondencia electrónica	20 // 22 21 // 19
255	Alteración de evidencia informática	7 // 8 104 // 151
157 157bis	Revelación de secretos Afectación datos personales	7 +4 // 6 +5 12 // 4
153bis	Acceso ilegítimo a sistema o dato informático	12 // 9 21 // 29
155 173	Pub. indebida de comunics Estafa informática	3 // 2 0 // 0
128	Distribución o comercio de pornografía infantil	3 // 0 694 // 871

(20) La tercera columna indica a la derecha los casos de 2013 y a la izquierda los de 2014, el primer renglón corresponde a datos del fuero federal y el segundo a los de la Provincia de Bs. As.

(21) La tercera columna indica a la derecha los casos de 2015 y a la izquierda los de 2016, el primer renglón corresponde a datos del fuero federal (y precedido con "+" los de la Provincia de Bs. As. por ese mismo delito) y el segundo a los de la Provincia de Bs. As.

El cuarto cuadro nos permite visualizar que la tendencia iniciada en 2014 se disparó con el notable incremento de casos en la Provincia de Buenos Aires por presuntas infracciones al artículo 128 del Código Penal, lo que no solo lo ubica otra vez como el tipo penal por el que se hacen más denuncias sino que supera solo a la totalidad de los restantes: 697 casos en conjunto para 2015 y 871 en 2016.

Puede acotarse que la desaparición paulatina de casos por esta tipicidad en el fuero federal vino acompañada de la transferencia de competencias al fuero ordinario de la Ciudad Autónoma de Buenos Aires (CABA). En ella, donde se asignó a Unidades Fiscales Especializadas la investigación de los casos de delincuencia informática[22], se advierte que se alcanzaron cifras de denuncia muy significativas en el caso del artículo 128 del Código Penal. Es lo que ilustra el cuadro siguiente.

Cuadro 5

CABA FUERO ORDINARIO	DENUNCIAS	128	153BIS	183
2014	1288	1197 1° 965 2° 226 3° 5	70	21
2015	3247	3168 1° 3153 2° 12 3° 3	74	32
2016	1836	1729 1° 1706 2° 16 3° 7	76	31

Queda entonces claro que en los años que se analiza (2014-2016), en CABA, los fiscales especializados han concentrado casi su total atención en casos por presuntas infracciones a los párrafos primero, segundo o tercero del artículo 128 del Código Penal (en la columna correspondiente el primer dato es el general y luego se observa el desglose). Mientras que las denuncias por los artículos 153 bis y 183 fueron sensiblemente menores. No obstante el abrupto descenso de 2015 a 2016, en este último año más que duplicó el número de casos de la Provincia de Buenos Aires (1729 vs. 871; el año anterior fue superior al triple: 3168 vs. 694).

Dejando el sesgo de interés local, a nivel mundial, ya en 2010 organizaciones no gubernamentales especializadas denunciaban que con las voces *"child pornography"* se estaban haciendo alrededor de 116.000 búsquedas diarias en los buscadores más conocidos de material en Internet[23]. La NHC, organización no gubernamental del

(22) Así, la Fiscalía PCyF N° 12, a cargo de la doctora Daniela S. Dupuy (cf. http://www.fiscalias.gob.ar). En el ámbito de la Procuración General de la Nación también se ha conformado una Unidad Fiscal Especializada en Ciberdelincuencia (UFECI), a cargo del doctor Horacio J. Azzolin (cf. http://www.fiscales.gob.ar)

(23) Se suele citar como fuente el tráfico registrado en portales como "Pornhub"

Reino Unido dedicada a la protección de la infancia, ha revelado estadísticas que indican que los delitos relacionados con la pornografía infantil, gracias a Internet, se han incrementado un 1500% desde 1988[24]. Hay quien, incluso, aventura la detección de un nuevo tipo de "delincuente sexual", que establece contacto con un niño por medio de Internet *"y está dispuesto a recorrer distancias quizás enormes, a través de Estados, continentes y países, a fin de encontrarse con el niño y abusar sexualmente de él"*.[25]

Cerrando entonces este recordatorio estadístico, no debe soslayarse que el período que se ha focalizado es uno en el que la nueva tipicidad, la tenencia simple, no estaba prevista y habrá que ver en los próximos años si se genera algún tipo de cambio de significación a partir de esta inclusión.

IV - TIPO OBJETIVO

Pasamos ahora al análisis dogmático del texto del artículo 128 del Código Penal transcripto en la introducción.

a) Verbo típico

El artículo establece en sus párrafos distintos tipos penales que, además, siguiendo una práctica asumida por el legislador en otras ocasiones, utilizan una sucesión de verbos típicos con los que procura alcanzar todo lo que configuraría la cadena de elaboración y comercialización de la pornografía infantil. Así, las diferentes acciones son presentadas como una secuencia o conformando una suerte de cascada en la que, sin importar el momento o eslabón en que se detenga la actividad, a todo se lo conmina con la misma pena en abstracto. Pasemos al detalle:

a.1) En el primer párrafo se punen las acciones *de producir, financiar, ofrecer, comerciar, publicar, facilitar, divulgar o distribuir*, por cualquier medio, imágenes pornográficas de menores de 18 años, así como organizar espectáculos en vivo de aquel tenor en que participen menores.

Adviértase que la última parte, vinculada a la organización de espectáculos, bien podría haber sido un párrafo separado ya que no guarda la estrecha vinculación que tienen los otros verbos que le preceden al no relacionarse con una actividad en vivo y directo. En todos los casos, se trata de tipo activo, de resultado e instantáneo, de pluralidad de actos, también denominado mixto alternativo.[26]

Referencia jurisprudencial de interés: la Sala I de la Cámara Nacional de Apelaciones en lo Criminal y Correccional, ha señalado que *"la figura de la distribución de imágenes pornográficas de menores de dieciocho años de edad que regula el artículo 128, segundo párrafo del Código Penal, castiga la distribución de imágenes pornográficas de menores de dieciocho años de edad y no el mero hecho de recibir este tipo de fotografías. Es necesario no solo recibir, sino además, enviar a otras personas imágenes pornográficas*

(24) Cf. informa Rico, Martín en su trabajo: "La interpretación del art. 2 de la ley 26388 a la luz de las recomendaciones internacionales en materia de ciberdelitos" - Suplemento de Derecho y Altas Tecnologías - Biblioteca Jurídica online el Dial.com - edición del 13/6/2008

(25) Cf. Vázquez, Marcelo P. en su trabajo: "La explotación sexual comercial de la niñez y su relación con la red Internet" - CDJP - Ad-Hoc - Nº 18-19 - Bs. As. - 2005, en su trabajo citado en nota 17, págs. 644/5

(26) Arocena, Gustavo A.: "Ataques a la integridad sexual" - Ed. Astrea - Bs. As. - 2012 - pág. 107

de menores de edad. Aquí también es importante señalar que la descripción penal alude a la voz distribución de imágenes, hecho este que descarta el mero envío de textos solo referidos a ella".[27]

Por lo pronto, es claro que las tecnologías de la información y la comunicación (TIC) han dado lugar al surgimiento de nuevas formas de intercambio y obtención de representaciones sexuales de menores. Van desde la difusión mediante la creación de páginas web (primera fase), la aparición de los "clubes de pornografía infantil" (segunda fase) y la información, captación, publicidad y puesta en contacto con el cliente consumidor de materiales o servicios (tercera fase) -sin desconocer que convive junto al comercio un fenómeno asociativo informal y sin ánimo de lucro económico-[28]; así como *"otros modos de satisfacer o incitar las inclinaciones sexuales con menores a través de la red, generando un amplio debate en torno a su criminalización, al entenderse como propiciadoras o favorecedoras de la explotación sexual infantil, pues la estimulan o justifican: la pornografía infantil técnica, la pseudopornografía infantil, la pornografía infantil virtual, la apología de la pornografía o de la pedofilia, etc."*.[29]

Fernando Miró Llinares resalta que en la actualidad la principal fuente de producción de pornografía es la red, pero a través de organizaciones criminales internacionales con finalidad de lucro que realizan su actividad por medio de asociaciones o empresas encubiertas que operan con nota de permanencia. El beneficio económico deriva de que se cobra al destinatario dinero como contraprestación por el material pornográfico: luego de abonado, se recibe la clave de acceso a la página web o se le remiten los archivos con las imágenes requeridas[30]. Agrega que en términos de nacionalidades de los niños victimizados, se trata de conductas muchas veces vinculadas a otros ilícitos como el problema del turismo sexual y el tráfico de personas. Dentro de este grupo, indican algunos informes la importancia de países de la ex Unión Soviética. En cambio, cuando se trata de material distribuido en DVD o formatos similares, los protagonistas suelen ser menores de zonas del tercer mundo y Asia. A su vez, en la pornografía que circula por internet se observa cierta preeminencia de víctimas de Tailandia u otros países de la misma zona asiática.[31]

a.2) En el segundo y tercer párrafos se introducen como típicas la tenencia o posesión de tales representaciones con distintas finalidades. En el nuevo segundo párrafo, conforme la reciente reforma por ley 27436, se consagra la denominada "tenencia o

(27) "N., G. A." - 25/4/2002, causa 18108, citado por Donna, De la Fuente, Maiza y Piña, en su obra: "El Código Penal y su interpretación en la jurisprudencia" - Ed. Rubinzal-Culzoni Editores - Bs. As./Santa Fe - 2003 - T. II, arts. 79 a 161 - pág. 630. Allí, puede consultarse la síntesis del caso "M., E." de la Sala V del mismo tribunal (16/10/2002, causa 19902), que sobreseyó respecto de la conducta de distribución sobre la base de entender que pune algo más que el simple envío a un destinatario, sino que presupone un número indeterminado de receptores, el que fuera revocado por prematuro por la Sala 1 de la CN Casación Penal

(28) Ruiz Rodríguez, Luis R. y González Agudelo, Gloria: "El factor tecnológico en la expansión del crimen organizado", en AA. VV.: "Criminalidad organizada, terrorismo e inmigración. Retos contemporáneos de política criminal" - Ed. Comares - Granada - 2008 - págs. 25/7

(29) Ruiz Rodríguez, Luis R. y González Agudelo, Gloria: "El factor tecnológico en la expansión del crimen organizado", en AA. VV.: "Criminalidad organizada, terrorismo e inmigración. Retos contemporáneos de política criminal" - Ed. Comares - Granada - 2008 - pág. 24

(30) Miró Llinares, Fernando: "El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio" - Ed. Marcial Pons - Madrid - 2012 - pág. 112

(31) Miró Llinares, Fernando: "El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio" - Ed. Marcial Pons - Madrid - 2012 - pág. 113

posesión simple", mientras que en el ahora desplazado como tercero se contempla aquella con fines inequívocos de distribución o comercialización. La nota de "inequivocidad" es producto acertado de la intervención de la llamada Cámara "vieja", ya que la de Diputados no había incluido tal precisión.

Refiriéndonos al texto ahora sustituido[32], habíamos señalado nuestra coincidencia con la acertada observación de Hugo A. y Gustavo J. Vaninetti sobre la necesidad de un debate acerca de la eventual incorporación de las figuras de posesión simple de material pornográfico infantil y posesión preordenada para venta, distribución o exhibición de material pornográfico infantil. La contradicción abierta entre la reserva y la sanción de la ley modificatoria del artículo en comentario revela que algunos antecedentes de aquella no se han reafirmado y el debate de la nueva dirección no ha sido realmente abierto, más allá de conocerse que desde el ámbito del Ministerio Público Fiscal de la CABA, con sus fiscales especializados en la materia, se reclamaba por la incorporación de esta tipicidad. Puede anotarse que la utilización a sabiendas tendería a reforzar la idea de que lo ingresado al área punible es una tenencia que se ejerce con dolo directo y que, por lo tanto, quedarían afuera ocasionales recepciones no requeridas ni expresamente guardadas o no percibidas claramente como aquellos materiales prohibidos referidos.

El tercer párrafo del tipo actual recoge la previsión del Protocolo aprobado por ley 25763, cuyo artículo 3 dispone: *"Todo Estado parte adoptará medidas para que, como mínimo, los actos y actividades que a continuación se enumeren queden íntegramente comprendidos en su legislación penal, tanto si se han cometido dentro como fuera de sus fronteras, o si se han perpetrado individual o colectivamente ... c) La producción, distribución, divulgación, importación, exportación, oferta, venta o posesión, con los fines antes señalados, de pornografía infantil".*[33]

Similar y aun con una mayor amplitud en el derecho comparado puede citarse el artículo 189.1.b. y 189.5 del Código Penal español, conforme modificación introducida por LO 1/2015 de 30 de marzo, que dicen:

> *"189.1. Será castigado con la pena de prisión de uno a cinco años: ...*
>
> *b) El que produjere, vendiere, distribuyere, exhibiere, ofreciere o facilitare la producción, venta, difusión o exhibición por cualquier medio de pornografía infantil o en cuya elaboración hayan sido utilizadas personas con discapacidad necesitadas de especial protección, o lo poseyere para estos fines, aunque el material tuviere su origen en el extranjero o fuere desconocido ...*
>
> *5. El que para su propio uso adquiera o posea pornografía infantil o en cuya elaboración se hubieran utilizado personas con discapacidad necesitadas de especial protección, será castigado con la pena de tres meses a un año de prisión o con multa de seis meses a dos años.*
>
> *La misma pena se impondrá a quien acceda a sabiendas a pornografía infantil o en cuya elaboración se hubieran utilizado personas con discapacidad necesitadas de especial protección, por medio de las tecnologías de la información y la comunicación".*

(32) En Riquert, Marcelo A.: "Comentario al art. 128, CP", en AA. VV.: "Código Penal y normas complementarias. Análisis doctrinal y jurisprudencial", Zaffaroni, Eugenio R. y Baigún, David (Dirs.) - 2ª ed. - Ed. Hammurabi - Bs. As. - 2010 - T. 4 - pág. 735 y ss.

(33) Cf. Vaninetti, Hugo A. y Vaninetti, Gustavo J.: "La posesión simple y preordenada de material con pornografía infantil. Internet: su incidencia. Necesidad de una doble inclusión en el Código Penal" en "El derecho penal. Doctrina y jurisprudencia" - ED - Nº 7 - julio/2007 - págs. 6/12

Es decir que se incluye con pena de forma atenuada no solo la distribución o venta (1.b) sino la mera adquisición o posesión para uso propio, además del acceso a sabiendas al material prohibido (5). La mayor amplitud afirmada deviene de la inclusión de la adquisición y el acceso a sabiendas, mientras que la norma nacional se ciñe a la posesión o tenencia, ya sea simple o con fines de venta o distribución.

Se ha argumentado que si bien ofrece como dificultad la de probar estas últimas preordenaciones, esto es un problema de índole procesal que en nada obstaculiza la razonabilidad del tipo. Sin embargo, justamente esta dificultad solía enarbolarse como un ejemplo de la pérdida de eficacia en la persecución penal cuando no podía acreditarse la ultraintención si no solo la mera tenencia del material prohibido, de lo que se concluía en la necesidad de incluir la última para evitar el problema.(34)

Volviendo entonces a la simple posesión, habíamos señalado cuando fuera la reforma por ley 26388 que ciertamente se trata de un tipo que merece un debate amplio. Por un lado, conlleva el problema de la polémica acerca de su posible incursión en ámbitos de reserva de moral sexual en equiparación con otras conductas mucho más graves y de directa lesividad(35) y, por otro, no difiere demasiado del genérico alrededor de las figuras de "tenencia" punibles y los delitos de peligro abstracto, que excede el objeto de este trabajo(36). Martín Rico sostuvo antes de la reforma que al no incorporar la ley como supuesto típico, este orden de tenencias estaría obedeciendo a lo normado en el artículo 19 de la CN (principio de reserva), por lo que *"no estaría cometiendo delito quien navega en páginas que contienen pornografía infantil"*(37). Con ella, siendo que lo tipificado es la tenencia bajo propio poder a sabiendas, este aspecto parece no haber cambiado. En cambio, no escaparía a la tipicidad de la norma española transcripta, que incluye el acceso a sabiendas.

Dupuy sistematiza los argumentos en contra de la penalización de la simple posesión en los siguientes: a) vulneración del principio de mínima intervención; b) adelantamiento de las barreras del derecho penal: delitos de peligro abstracto; c) intromisión en la vida privada de los adultos y d) moral social colectiva (derecho penal de autor)(38). A su vez, los argumentos a favor son: a) controlar la demanda para anular la oferta; b) peligro de acciones imitadoras por los usuarios; c) empatía con las víctimas de la pornografía infantil; d) riesgo social y vinculación entre quienes consumen pornografía infantil y los abusos sexuales posteriores.(39)

(34) Así, Dupuy, Daniela: "La posesión de pornografía infantil", en AA. VV.: "Cibercrimen", bajo su propia dirección - Ed. BdeF - Montevideo/Bs. As. - 2017 - pág. 138

(35) Cf. Ruiz Rodríguez, Luis R. y González Agudelo, Gloria: "El factor tecnológico en la expansión del crimen organizado", en AA. VV.: "Criminalidad organizada, terrorismo e inmigración. Retos contemporáneos de política criminal" - Ed. Comares - Granada - 2008 - pág. 22

(36) Sobre el particular nos extendimos en el trabajo "La punición de la tenencia de pornografía infantil en la Argentina", en AA. VV.: "Delitos de posesión o tenencia", Friedrich-Christian Schroeder, Ken Eckstein y Andrés Falcone (Coords.) - Ed. Ad-Hoc - Bs. As. - 2016 - págs. 371/93

(37) Rico, Martín en su trabajo: "La interpretación del art. 2 de la ley 26388 a la luz de las recomendaciones internacionales en materia de ciberdelitos" - Suplemento de Derecho y Altas Tecnologías - Biblioteca Jurídica online el Dial.com - edición del 13/6/2008 - pág. 2

(38) Dupuy, Daniela: "La posesión de pornografía infantil", en AA. VV.: "Cibercrimen", bajo su propia dirección - Ed. BdeF - Montevideo/Bs. As. - 2017 - págs. 128/31

(39) Dupuy, Daniela: "La posesión de pornografía infantil", en AA. VV.: "Cibercrimen", bajo su propia dirección - Ed. BdeF - Montevideo/Bs. As. - 2017 - págs. 131/4

Coincido con Reinaldi que al cambiar el bien jurídico, la publicidad deja de ser un requisito del tipo penal, bastará para que el delito se consume con la realización de las acciones típicas. Se utiliza menores como objeto y, por ende, se los deshumaniza.(40)

a.3) Por último, el cuarto párrafo tipifica la *facilitación* de acceso al menor a *ver espectáculos pornográficos o el suministro* de material de ese cariz.

Un tema interesante que plantea este párrafo cuando pune el "suministro" de material pornográfico a menores de 14 años es mencionado por Pont Vergés, quien entiende que esta acción alcanza a quienes crean y mantienen un sitio web (proveedores de contenidos), que pone a disposición del público en general material pornográfico, siempre que no tomen los recaudos plausibles para que los menores de 14 años no ingresen a ellos. Recuerda, además, en cuanto a los ISP, la vigencia de la ley 25690 que les obliga a ofrecer software de protección (filtros) que impida el acceso de menores a sitios específicos para adultos, al momento de prestar su servicio.(41)

a.4) Para cerrar este punto, si se hace un rápido repaso de las modificaciones más significativas introducidas mediante la ley 26388, deben destacarse las siguientes:

a.4.1) Se pasó de no mencionar ningún medio de concreción para las acciones típicas a explicitar que puede serlo cualquiera.

a.4.2) El elenco de conductas típicas anterior ("produjere", "publicare", "distribuyere" y "organizare", de sus primeros dos párrafos) se concentró en el primer párrafo actual, en el que se agregaron las de "financiare", "ofreciere", "comerciare", "facilitare" y "divulgare".

a.4.3) Con pena atenuada se incorporó en el nuevo segundo párrafo la conducta de *"tenencia ... con fines inequívocos de distribución o comercialización"* de las representaciones pornográficas de menores.

Ahora, con la ley 27436, se agrega la incorporación de la tenencia simple de tales representaciones.

b) Otros elementos del tipo objetivo

El primer párrafo de la norma nos ayuda, en una interpretación sistémica, para comprender el último del artículo en estudio, toda vez que se reemplaza el concepto de lo "obsceno" (como lo establecía el texto originario de 1921), por lo "pornográfico". Si bien ambos conceptos resultan ser ambiguos, a la hora de encontrar un concepto normativo satisfactorio que exige la ley penal debemos recordar que el primer párrafo establece *"actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales"*, lo que, como primera aproximación diferencial, implica un requerimiento de mayor grado de intensidad que el texto anterior. Se alude a que esas imágenes (pinturas, fotografías, películas) deben tener contenido de sexo explícito y no meramente de carácter sexual u obsceno. Debe tratarse de imágenes de menores de 18 años de edad, lo que se conoce como "pornografía infantil".

(40) En su obra "Los delitos sexuales en el Código Penal argentino. Ley 25087" - Marcos Lerner Editora - Córdoba - 1999 - pág. 211

(41) Pont Vergés, Francisco en su trabajo: "¿Debe prohibirse y sancionarse penalmente la divulgación de pornografía?" - Suplemento de Derecho y Altas Tecnologías - Biblioteca Jurídica online el Dial.com - edición del 12/9/2007 - pág. 8

Pero, insistimos, se afronta la siempre difícil determinación conceptual de elementos normativos de enorme porosidad e imprecisión que llevan este tipo de figuras, como qué debe entenderse justamente por "pornografía infantil". En un anterior trabajo[42], hemos señalado que, para un sector de la doctrina, habiendo quedado fuera la pornografía entre y para adultos, podría entenderse que algo del problema se ha minimizado. Así, Fernando M. Bosch recuerda que la Corte Suprema estadounidense, en el caso "New York c/Ferber", de 1982, resolvió que la pornografía infantil no requería siquiera ser legalmente calificada como obscena antes de ser prohibida[43]. Sobre lo correcto de aquella limitación, tan postergada, puede recordarse que ya decía a comienzos de la década de los sesenta Jiménez de Asúa: *"Me parece una pretensión absurda tratar de obligar a gente adulta a que vea o deje de ver lo que a una ley, a un fiscal, a un juez o a un censor se le antoje ordenar o prohibir ... El único problema, a mi juicio, es el de los menores: la protección de la moralidad, del pudor y de la honestidad de quien aún no es adulto"*.[44]

Por su parte, Zulita Fellini señala que la pornografía infantil equivale a la utilización abusiva del niño y que puede llevar a otras formas de explotación, entendiéndose por tal *"la representación visual o auditiva de un niño para el placer sexual del usuario, y entraña la producción, la distribución o el uso de ese material"*. Aclara que la expresión "utilización de niños en la pornografía" dio paso a varias interpretaciones, entre las que destaca las siguientes: *"todo material audiovisual que utilice a los niños en un contexto sexual"* y *"una representación permanente de un menor de 18 años en un acto sexual explícito, real o simulado, o la exhibición obscena de sus órganos genitales. Se incluye en el acto sexual explícito, sin quedar limitada a ellas, las siguientes operaciones: relación vaginal, relación anal, fellatio, cunnilingus y analingus"*.[45]

Más allá de que podrían enumerarse cantidad de opiniones y conceptos, en nuestro derecho se ha entendido en tiempos recientes que el alcance jurídico del concepto de pornografía infantil viene delineado por la ley 25763[46], cuyo artículo 1 aprueba el *Protocolo facultativo de la Convención sobre los Derechos del Niño relativo a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía* (Asamblea General de Naciones Unidas, sesión plenaria del 25/5/2000). El artículo 2, inciso c), dice que *"por pornografía infantil se entiende toda representación, por cualquier medio, de un niño dedicado a actividades sexuales explícitas, reales o simuladas, o toda representación de las partes genitales de un niño con fines primordialmente sexuales"*.

(42) En la obra de Riquert, Marcelo A.: "Delincuencia informática en Argentina y el Mercosur", prologada por el doctor David Baigún - Ed. Ediar - Bs. As. - 2009

(43) Bosch, Fernando en su trabajo: "Las publicaciones obscenas, la pornografía y un fallo ejemplar" - LL - T. 1986-D - pág. 441

(44) Jiménez de Asúa, Luis: "La protección penal del pudor público", en "El Criminalista", 2ª serie, Víctor P. de Zavalía - Bs. As. - 1961 - T. V. - págs. 146/7

(45) En su trabajo "Comentarios a la ley 25087 sobre 'Delitos contra la integridad sexual'. Modificaciones al Código Penal" - LL - Actualidad, diario del 25/11/1999. La cita corresponde a págs. 2/3

(46) BO: 25/8/2003

Si bien ya se llamó la atención sobre esto, vale aquí insistir en la inclusión expresa de las simulaciones de acto sexual explícito de un menor. Destaca Palazzi, con referencia al trámite parlamentario de la ley 26388, que el texto de Diputados incluía las actividades "simuladas", que fueron excluidas en Senadores por considerárselo un tema controvertido pese a su previsión por el Protocolo citado[47]. Ciertamente, es una cuestión espinosa: en la medida en que se hiciera públicamente, rápido surgirá la dificultad de deslindar límites entre libertad de expresión/manifestación artística y simple apología del delito, en general reprimida por el artículo 213 del Código Penal.

c) Sujeto activo

Puede ser cualquier persona que realice las conductas establecidas en la norma, por lo que se trata de un delito común, siendo de aplicación las reglas generales de la participación. No se ha contemplado agravante por la calidad del autor (por ejemplo, el padre, tutor, curador, etc.).

En algunas de las conductas descriptas, singularmente en la "distribución", no debe soslayarse que por la arquitectura de la red resulta evidente la posible intervención responsable de personas jurídicas[48]. Vale la pena recordar que, dentro del frondoso articulado del Ciberconvenio aprobado (48 en total) conviven previsiones de naturaleza sustancial y procesal. Dentro del Capítulo II, que especifica las "Medidas que deben ser adoptadas a nivel nacional", la Sección 1 se dedica al "Derecho penal material" y, dentro de ella, el Título 5 se refiere a "Otras formas de responsabilidad y sanción". Allí están radicadas las normas que singularmente interesan sobre este punto. En efecto, el artículo 12[49] fija las pautas en orden a la responsabilidad de las personas jurídicas, admitiendo

(47) En el trabajo "Análisis de la ley 26388 de reforma al Código Penal en materia de delitos informáticos" - Revista de Derecho Penal y Procesal Penal - Ed. LexisNexis - N° 7/2008 - Bs. As. - pág. 1214

(48) Concuerda en destacar este aspecto Aboso, Gustavo E.: "Derecho penal cibernético" - Ed. BdeF - Montevideo/Bs. As. - 2017 - págs. 222/6

(49) Su texto dice: *"Art. 12 - Responsabilidad de las personas jurídicas. 1. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para permitir que las personas jurídicas puedan ser tenidas por responsables de las infracciones establecidas en el presente Convenio, cuando estas sean cometidas por una persona física, actuando ya sea a título individual, ya sea como miembro de un órgano de la persona jurídica, que ejerce un poder de dirección en su seno, cuyo origen se encuentre en:*

a) un poder de representación de la persona jurídica;

b) una autorización para tomar decisiones en nombre de la persona jurídica;

c) una autorización para ejercer control en el seno de la persona jurídica.

2. Fuera de los casos previstos en el párrafo 1, las Partes adoptarán las medidas necesarias para asegurar que una persona jurídica puede ser tenida por responsable cuando la ausencia de vigilancia o de control por parte de cualquier persona física mencionada en el párrafo 1 haya permitido la comisión de las infracciones descritas en el párrafo 1 a través de una persona física que actúa bajo autorización de la persona jurídica.

3. La responsabilidad de la persona jurídica podrá resolverse en sede penal, civil o administrativa, dependiendo de los principios jurídicos propios del Estado.

4. Esta responsabilidad se establecerá sin perjuicio de la responsabilidad penal de las personas físicas que hayan cometido la infracción"

posibles respuestas de naturaleza civil, administrativa y penal, en todos los casos con independencia de las que pudieren corresponder a las personas físicas que hubieren cometido la infracción, y el 13, numeral 2[50], referido a las sanciones correspondientes.

Lo primero que surge claro es que no habría, en realidad, déficit evidente para el derecho interno por la carencia de normas penales específicas, ya que el parágrafo tercero del artículo 12, respetuoso de las posibles diversas configuraciones de los principios jurídicos que rigen en los países signatarios, admite que cuando se demanda por la responsabilidad de las personas jurídicas, esta pueda ser civil, administrativa o penal. Además, conforme el parágrafo siguiente, aquella responsabilidad para los entes ideales lo es sin perjuicio de la penal que correspondiere a las personas físicas que hubieran cometido la infracción (el llamado principio de independencia de acciones).

Pero no menos claro, es evidente la singular importancia que, en la estructura y configuración de la red telemática, tienen los prestadores de servicio (en sus diferentes clases: estructura, acceso, alojamiento y contenidos), que no son otra cosa que grandes empresas que, a la vez que se benefician, tienen una cierta cuota de responsabilidad (corresponsabilidad) en el control de asuntos, objetos o servicios ofrecidos cotidianamente por Internet. Como dicen Aboso y Zapata, estamos frente a una situación que obliga a replantearse la responsabilidad penal de las personas de existencia ideal, en muchos países sistemáticamente negada al calor del viejo aforismo *"societas delinquere non potest"*[51]. No es esta la ocasión de profundizar esto, pero quisiera dejar constancia de algunos matices de importancia para dar en el futuro cercano esta discusión.[52]

En la Argentina no hay previsión de carácter general que fije la responsabilidad penal de las personas jurídicas, lo que ha llevado a un sector muy importante de la doctrina y la jurisprudencia a sostener la vigencia del citado adagio. Sin embargo, una miríada de dispersas disposiciones prevén desde hace mucho tiempo penas a imponer en sede penal como consecuencia de distintas actividades delictivas. En diciembre/2017, se sancionó la ley 27401 por la que se estableció un régimen de *"responsabilidad penal de las personas jurídicas"* en delitos contra la administración pública y el cohecho nacional y transnacional. Por eso, entiendo que, al menos parcialmente, rige al presente el *"societas delinquere potest"*.

(50) Art. 13 - *"Sanciones y medidas. 1. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para permitir que las infracciones penales establecidas en los artículos 2 a 11 sean castigadas con sanciones efectivas, proporcionadas y disuasorias, incluidas las penas privativas de libertad.*

2. Las Partes velarán para que las personas jurídicas que hayan sido declaradas responsables según lo dispuesto en el artículo 12 sean objeto de sanciones o medidas penales o no penales efectivas, proporcionadas y disuasorias, incluidas las sanciones pecuniarias"

(51) Aboso, Gustavo E. y Zapata, María F.: "Cibercriminalidad y derecho penal" - Ed. BdeF - Bs. As. - 2006 - pág. 211. Puede agregarse que, usualmente presentado como originario del derecho romano, el "societas delinquere non potest" es atribuido por autores como De la Cuesta Arzamendi a Sinibaldo de Fieschi (luego, Papa Inocencio IV), en el siglo XIII. También Tiedemann sostiene la dudosa genuinidad histórica del aforismo, indicando que la punición de las asociaciones era habitual en Europa hasta la Revolución Francesa

(52) Corresponden a la ponencia titulada "La responsabilidad penal de las personas jurídicas y el Ciberconvenio de Budapest", que presentara recientemente en el marco del panel "Tendencias modernas en el derecho penal", en ocasión del XVIII Encuentro de Profesores de Derecho Penal y VIII Jornadas Nacionales de Derecho Penal, organizado por la Asociación Argentina de Profesores de Derecho Penal y la Universidad Nacional de Cuyo - Mendoza - 10 y 11/5/2018

Dentro del catálogo de delitos en los que la respuesta penal está habilitada puede encontrarse alguno constitutivo de la delincuencia informática, como la alteración dolosa de registros fiscales o previsionales, tanto documentales como informáticos, y de sistemas informáticos o equipos electrónicos suministrados, autorizados u homologados por el Fisco (art. 11, L. 27430, reciente régimen penal tributario y previsional); evidente atentado contra la integridad de datos o de sistemas conforme artículos 4 y 5 del Ciberconvenio. Es claro que hay muchas otras infracciones a este último en las que la intervención de los "proveedores de servicios" de Internet (ISP) o los "buscadores" que facilitan el acceso a los contenidos asumen una entidad/gravedad por vía activa u omisiva que sería apropiado incluirlas dentro de aquel grupo. Se trata, sin duda, de una importante tarea pendiente.(53)

En el artículo 12 del Ciberconvenio se identifican dos fuentes de atribución de responsabilidad para la persona jurídica: 1. la actuación de una persona física que ejerce un poder de dirección en el seno de la persona jurídica, ya sea que lo haga a título individual o como miembro de uno de sus órganos, siendo que se le hubiere dado poder de representación o autorización para la toma de decisiones o ejercicio de control del ente ideal; 2. la ausencia de vigilancia o control de esa persona física antes mencionada que hubiere permitido la comisión de la infracción a través de una persona física que actúa bajo autorización de la persona jurídica. Ceñido el cotejo a las tres normas nacionales más recientes, se advierte que los criterios que habilitan la atribución de responsabilidad y la consiguiente posibilidad de sancionar son en estas de mayor amplitud: cuando el hecho hubiere sido realizado en nombre, o con la intervención, o en beneficio de una persona de existencia ideal (art. 304, CP), o un ente que a pesar de no tener calidad de sujeto de derecho las normas le atribuyan condición de obligado (art. 13, L. 27430). Más aún, se incluye la hipótesis "en beneficio", aunque el hecho no se realizare en su nombre o con su intervención por un tercero carente de atribuciones, cuando la persona jurídica hubiera ratificado su gestión aunque sea en forma tácita (art. 2, L. 27401).

En cuanto a la omisión de vigilancia sobre la actividad de los autores y partícipes, en la legislación nacional es un factor más de graduación de la pena. En la ley 27401, por primera vez en nuestro derecho, se incluye la posible valoración como eximente de pena de la implementación por la persona jurídica de un programa de cumplimiento normativo o de "integridad" (*compliance*). De extenderse esta decisión político-criminal sobre la posible exención de pena que incluye a la de orden administrativo, pero no a la civil, no habría colisión con el Ciberconvenio, no solo porque deja abierta la última posibilidad, sino también porque la adopción del programa de integridad demuestra que no se trata de un supuesto de ausencia de vigilancia o control atribuible a la empresa.

Luego de un muy largo derrotero, producto de un complejo proceso de interacción entre jurisprudencia y doctrina, tanto en el ámbito internacional como local, al presente y más allá de matices en el nivel de detalle, suelen identificarse como estándares para responsabilizar a los ISP o a los buscadores por contenidos ajenos ilícitos, dos factores, a saber: a) el conocimiento de la ilicitud o la existencia de hechos manifiestamente reveladores; b) que habiendo sido denunciado conforme el procedimiento legal interno el

(53) Gustavo Sain, en cuanto apunta que en ocasión de la reforma por L. 26388 no se previó en forma expresa para ninguna de las nuevas tipicidades que establecía que mediare responsabilidad de los proveedores de servicio de Internet (en su obra conjunta con Azzolin, Horacio: "Delitos informáticos. Investigación criminal, marco legal y peritaje" - Ed. BdeF - Montevideo/Bs. As. - 2017 - pág. 80)

contenido, no se hubiere adoptado un obrar diligente para retirarlo[54]. Derivado de ello, no debería admitirse la responsabilidad penal por omisión intencional de aquellos si no existe alguna disposición legal que obligue a controlar contenidos determinados de manifiesta ilicitud en forma preventiva antes de hacerlos accesibles y que dicho control sea razonablemente posible.[55]

Por último, en torno a la obligación de control de contenidos (suerte de la función de policía o gendarme de la red que no debiera delegarse absolutamente en los privados), la idea básica que transmiten las leyes 26032 y 27078 es que no hay para los ISP un deber general de supervisión o vigilancia[56]. La mencionada premisa de "neutralidad" tiende a garantizar la libertad de expresión en la red. Cuando en casos como el de la ley 25690 se fija un deber de instalar o activar mecanismos técnicos de evitación de acceso a determinados sitios[57], se trata, como enfatiza Aboso, de una obligación que está supeditada al previo conocimiento fehaciente por parte de los titulares del servicio de la existencia de enlaces o sitios individualizados que promocionan o cometen actividades ilícitas[58]. Entonces, no se trata de supuestos de admisión de censura previa, sino de una restricción posterior derivada del conocimiento de la ilicitud.

(54) Cherñavsky le asigna al alerta previo del usuario o tercero perjudicado la función de una suerte de condición objetiva de punibilidad de la conducta del ISP: una vez que conoce el contenido injurioso, xenófobo, racista, de menoscabo de la integridad sexual de un menor, etc., el omitir el bloqueo generaría su responsabilidad civil y eventualmente penal por incumplimiento del deber de retirada frente a los contenidos antijurídicos ajenos, siguiendo el procedimiento que cada jurisdicción hubiera determinado para que actúe el proveedor [en su trabajo "¿Es posible responsabilizar penalmente a los proveedores de servicio de Internet?", en AA.VV.: "Cibercrimen", Dupuy, Daniela (Dir.) - Ed. BdeF - Montevideo/Bs. As. - 2017 - pág. 596]

(55) Cherñavsky, Nora: "¿Es posible responsabilizar penalmente a los proveedores de servicio de Internet?", en AA.VV.: "Cibercrimen", Dupuy, Daniela (Dir.) - Ed. BdeF - Montevideo/Bs. As. - 2017 - pág. 595

(56) En el ámbito de la CABA hay una situación particular con repercusión contravencional para el caso de los cibercafés o establecimientos comerciales que ofrecen servicios de Internet. Por ley 863/2002 tienen obligación de instalar en todas las computadoras a disposición del público filtros de contenido de sitios pornográficos cuando permitan que los usuarios sean menores de 18 años. Si los clientes son mayores, no media tal obligación y pueden desactivarse. La no instalación o su desactivación (con usuarios menores de 18 años) genera la posible imposición de multa de $ 200 a $ 1000 y/o clausura del local o comercio de hasta 5 días, cf. arts. 3.2.2 y 3.2.3 del Código de Faltas (Aboso, Gustavo E.: "Derecho penal cibernético" - Ed. BdeF - Montevideo/Bs. As. - 2017 - pág. 471)

(57) Francisco Pont Vergés deriva del art. 1, L. 25690 la obligación para los ISP de ofrecer software de protección (filtros) que impidan el acceso de menores a sitios específicos para adultos, al momento de prestar su servicio, asignándole posibles consecuencias de responsabilidad penal por "facilitación" de material pornográfico conforme el art. 128, CP (en su trabajo "¿Debe prohibirse y sancionarse penalmente la divulgación de pornografía?" - Suplemento de Derecho y Altas Tecnologías - Biblioteca Jurídica online el Dial.com - edición del 12/9/2007 - pág. 8). Sin embargo, la lectura de la norma invocada habla de filtros de un modo general, sin la especificidad indicada, lo que abriría paso a una posible discusión del caso particular. Para dilucidarlo cobrará particular significación el factor "conocimiento", según se explica en el texto principal

(58) Aboso, Gustavo E.: "Derecho penal cibernético" - Ed. BdeF - Montevideo/Bs. As. - 2017 - pág. 462

d) Sujeto pasivo

En el sujeto pasivo hay una razonable diferenciación, ya que las asimétricas modalidades de victimización lo justifican (se insiste desde esta perspectiva en la exigencia de actividad y la nota de pasividad que ofrecen los distintos segmentos del tipo). En definitiva, solo lo serán los menores de edad de 18 años con relación a la primera parte de la norma. El límite desciende a los de 14 años respecto de menores a los que se le facilitare el acceso a espectáculos pornográficos o le suministren material pornográfico (tercer párr.).

V - TIPO SUBJETIVO

En principio, estamos frente a un tipo penal doloso, no solo directo sino compatible con un posible dolo eventual. Cuestión que aparece conflictiva es el error acerca de la edad de los menores en las distintas figuras, toda vez que no existe la figura culposa.

Respecto del segundo párrafo, la inserción del "a sabiendas" es indicativa de que se trata de tenencia presidida por dolo directo.

Con relación al actual tercer párrafo, se verifica la exigencia de una ultraintencionalidad, ya que la tenencia demanda que sea con fines inequívocos de distribución o comercialización.

VI - CONSUMACIÓN Y TENTATIVA

Todas las conductas descriptas por la norma en su primero y último párrafos admiten en su *iter criminis* la tentativa, sin perjuicio de tratarse, en la mayoría, de los verbos típicos de un delito de mera actividad[59]. Situación diferente, por ejemplo, es la relativa a la publicidad o puesta en circulación de imágenes, filmaciones de menores establecidas en el primer párrafo. Allí, el delito se consuma una vez realizadas las tomas o filmaciones, sin necesidad de que se acredite su divulgación a terceras personas, más allá de las que participaron en la toma de las imágenes. Debemos recordar que lo que protege es la indemnidad sexual y la dignidad de los menores.

Si no fuesen casos de incriminación autónoma de acto preparatorio, el segundo y el tercer párrafos podrían constituir supuestos de tentativa cuando por razones ajenas a su voluntad se lo sorprende al distribuidor o comercializador con la tenencia del material pero aún no lo ha puesto en circulación o no alcanzó a venderlo.

De igual forma admitiría la tentativa el caso del menor al que se le facilita una revista con contenido pornográfico y no logra mirarla por razones ajenas a su voluntad (por ejemplo, vienen sus padres u otro mayor y le sacan el material). O el caso de la persona que le entrega al menor la entrada correspondiente para un espectáculo pornográfico, pero un tercero, que puede ser la persona encargada de recoger los boletos, exige la exhibición del documento de identidad y, por carecer de este o haberse verificado su real edad, se le impide la entrada.[60]

(59) En contra: Aboso, Gustavo E.: "Derecho penal cibernético" - Ed. BdeF - Montevideo/Bs. As. - 2017 - págs. 230/1; Sueiro, Carlos C.: "Criminalidad informática" - Ed. Ad-Hoc - Bs. As. - 2015 - págs. 92/5

(60) Ejemplo mencionado por Arocena, Gustavo: "Ataques a la integridad sexual" - Ed. Astrea - Bs. As. - 2012 - pág. 116. Concuerda en la posible tentativa para el cuarto párrafo Sueiro, Carlos C.: "Criminalidad informática" - Ed. Ad-Hoc - Bs. As. - 2015 - pág. 97

VII - CONCURSALIDAD

Según Donna, citando a Núñez y Creus, la multiplicidad de conductas del mismo sujeto sobre un mismo objeto no multiplica la delictuosidad, ya que se trata de un delito continuado.(61)

Las figuras descriptas admiten la posibilidad de concurso de delitos, ya sea ideal o real con otros que le preceden en el mismo título, como eventualmente con otras figuras vinculadas a la protección de la integridad física o de la libertad que pudieran conformar el marco en que se da el abuso de los menores.

VIII - PENA

Como se anticipó al momento de presentar los verbos típicos del primer párrafo, el problema básico de la pena conminada en abstracto (recordamos, seis meses a cuatro años de prisión) es que a toda la secuencia de conductas alternativas que allí se enuncian se le asigna idéntica escala y, realmente, cuesta ya no sostener sino entender cuál es la lógica de atribuir idéntico contenido de injusto a quien produce que a quien divulga, a quien ofrece que a quien financia. Valorativamente, ¿es lo mismo publicar unas imágenes pornográficas con intervención de menores que organizar un espectáculo de sexo en vivo con ellos?(62)

La tenencia simple del nuevo segundo párrafo comparte el mínimo de la del que le precedió (el hoy tercer párrafo) y tiene un máximo que es la mitad (un año). Si efectivamente solo tener es valorativamente menos que tener para distribuir o comercializar, el mínimo no debiera ser idéntico.

La otra reducción de pena, la del tercer párrafo, cuatro meses a dos años de prisión para la tenencia inequívoca con fines de distribución o comercialización, rompe con la tradición propia del régimen de estupefacientes (art. 5, L. 23737), donde la tenencia con fines es equiparada a la comercialización y la distribución. Digámoslo así, en este último régimen, esta particular tenencia se inserta en la secuencia del primer párrafo. Pareciera entonces que, al menos, aquí, al separarse y conminarse con distinta sanción, se supera el defecto apuntado respecto de aquel párrafo inicial. Sin embargo, no queda nada claro por qué el mínimo se reduce a dos tercios de aquella escala mientras que el máximo lo hace a la mitad. *¿Por qué esa desproporción?* Vale la pena aclarar que la reducción se debe al trámite en la Cámara de Senadores, ya que la de Diputados la preveía equiparada con la del primer párrafo (manteniendo el criterio ahora abandonado).

Y en cuanto al cuarto párrafo, la *facilitación* de acceso al menor de 14 años de edad a ver *espectáculos pornográficos* o el *suministro* de material de ese cariz (en ambos casos, se entiende que protagonizado por mayores) tienen también una reducción que aparece como lógica, toda vez que la actitud del menor frente al hecho pornográfico es pasiva -está en posición de observador- y no es el actor o partícipe del acto sexual,

(61) Donna, Edgardo A.: "Derecho penal. Parte especial" - Ed. Rubinzal-Culzoni Editores - Santa Fe - 1999 - T. I - pág. 167, donde cita de idéntico temperamento a Núñez y Creus

(62) Riquert, Fabián L. en su trabajo: "La ciberpornografía infantil en el Código Penal argentino", en AA. VV.: "Ciberdelitos", Riquert, Marcelo A. (Coord.) - Ed. Hammurabi - Bs. As. - 2014 - pág. 296

como en los supuestos anteriores. Ahora, frente a esta escala de un mes a tres de prisión, también luce incongruente que si el anticipo punitivo que importa la criminalización de la tenencia del segundo párrafo es considerado, en principio, tres veces más grave en su escala mínima (cuatro meses) que las conductas de facilitar y suministrar, esto también debiera haber tenido correlato en el máximo. Aclaramos que no estamos postulando incremento de pena, solo enunciando problemas de proporcionalidad que habría que solucionar.

IX - CONCLUSIÓN

El problema de la extensión del tráfico de material y producción de contenidos de pornografía vinculada a los menores se ha visto facilitado por las nuevas tecnologías de la información. A su vez, se vio reflejado, en los últimos tiempos, en el incremento de procedimientos judiciales internacionales sobre los que a diario dan cuenta diversos medios periodísticos. En todo caso, es claro que estamos frente a una actividad gravemente disvaliosa en la que la nota de globalización se ha acentuado justamente por la aparición de herramientas que permiten la configuración de verdaderas “redes delictivas”.

De los datos estadísticos aportados en el punto III del presente trabajo, no debe soslayarse que el período que se ha focalizado es uno en el que la nueva tipicidad, la tenencia simple, no estaba prevista y habrá que ver en los próximos años si se genera algún tipo de cambio de significación a partir de la nueva redacción del artículo 128 del Código Penal.

La pornografía infantil y la tenencia recientemente legislada

Daniela Dupuy(*)

I - INTRODUCCIÓN

Actualmente la pornografía infantil es un problema de dimensión internacional que se ha ramificado con el avance de las nuevas tecnologías, que permiten y facilitan la comisión de esta conducta delictiva, y que tornan insuficientes los programas de acción de los diferentes países del mundo para combatirla.

La eclosión de Internet ha revolucionado y facilitado el mercado de la pornografía infantil por varias razones:

- Disponibilidad económica de los usuarios para acceder a los equipos informáticos que posibilitan la captación y obtención de material de pornografía infantil.
- Abundancia de material pornográfico infantil que circula por la red, que facilita la interrelación entre el enorme número de aficionados y permite un intercambio constante de las fotografías, videos, películas, producciones, etc.
- Facilidad para descargar y compartir archivos con cero costos económicos, pues las técnicas de producción e introducción de dicho material en la red se ha multiplicado; comunicaciones y conversaciones interactivas por chat, por ejemplo, que permiten fácilmente poner a disposición videos y fotografías.
- La ventaja de permanecer en el anonimato. Intercambiar material de pornografía infantil detrás de la pantalla fomenta altamente el intercambio, la facilitación y la distribución del material, pues se desconoce el origen de la transmisión de los datos. El

(*) Abogada (UBA). Master in Law (Universidad de Palermo). Fiscal a cargo del equipo especializado de delitos informáticos de la CABA. Profesora adjunta en grado y posgrado de delitos informáticos (Universidad de Palermo). Docente de derecho procesal penal y contravencional de la CABA (Instituto Superior de Seguridad Pública)

usuario puede enmascararse en identidades ficticias o de imposible identificación y difundir contenidos a otro país, dificultando rastrear el origen desde donde se subió efectivamente el material pornográfico infantil.

- La posibilidad de acceder con mayor facilidad a los niños menores de edad a través de Internet, pues hoy las redes sociales representan una herramienta de comunicación natural y permanente para niños y adolescentes.
- La existencia de manuales de ayuda a pedófilos que permiten ayudarse mutuamente tanto para acceder al material que no encuentran, como así también para intercambiar consejos y advertencias para permanecer en el anonimato y no ser descubiertos por la justicia.

Estos aspectos explican el fuerte incremento en la distribución e intercambio de material pornográfico, que no se reduce a una finalidad comercial o de lucro sino con el objetivo de satisfacer las inclinaciones sexuales de los consumidores, con la consiguiente creación de redes internacionales de intercambio de pornografía infantil, que genera espacios que facilitan e incrementan la colección de fotografías y videos que los delincuentes suelen seleccionar y archivar en diferentes carpetas relacionadas con la edad, el sexo, el color de pelo de niños y niñas, desde una edad muy temprana -bebes de meses- hasta la adolescencia.

A lo expuesto debemos agregar la perpetuidad de la lesión al bien jurídico protegido -integridad sexual y libre desarrollo de la personalidad de los niños- pues tal accionar de circulación permanente del material prohibido en la red genera y asegura una continua distribución.

Miró Llinares(1) señala que no debemos desconocer las distintas fases por las que ha pasado la difusión de pornografía infantil a lo largo de los años hasta la irrupción de Internet.

Hace varios años existían páginas web alojadas en servidores de Internet, en las que el traficante comerciaba con el material pornográfico infantil que ponía a disposición de los usuarios, quienes previamente pagaban una contraprestación vía tarjeta de crédito del adquirente. En esta modalidad hay dos conductas: la de quien busca acceder a una determinada página web cuyo contenido sabe que contiene material pornográfico infantil; y la de quien crea la página de internet misma.

Luego aparecieron los chats en tiempo real, en los que los pedófilos dialogan y acuerdan intercambiarse a través de correo electrónico el material aludido. También la compra directa del material o la simple descarga de archivos. Luego los foros como medio de comunicación, el camuflaje de las páginas web de pornografía infantil que no se accedía a través de buscadores.

En poco tiempo, la figura del vendedor de pornografía infantil fue sustituida por la de consumidores que se asocian sin ánimo de lucro, bajando, subiendo y facilitando cantidad de archivos de contenido pornográfico infantil rápidamente y ayudados por las técnicas avanzadas de la tecnología *-red peer to peer-.*

Hoy la situación es incontrolable y es fundamental abordar la problemática desde la prevención, correcta legislación y sin dejar de observar el tratamiento en otros países, pues una de las características fundamentales de los delitos que se llevan a cabo en entornos digitales es la *transnacionalidad.*

(1) Miró Llinares, F.: "El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio" - Ed. Marcial Pons - 2012 - pág. 109

II - LEY 27436 DEL CÓDIGO PENAL

Recientemente el Congreso ha sancionado la ley que transforma en delito la mera tenencia de material de pornografía infantil.

La ley 27436 ha modificado el artículo 128 del Código Penal por el siguiente:

> **Art. 128 -** *"Será reprimido con prisión de tres a seis años el que 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".*

El artículo 9 de la Convención de Budapest, referente a la pornografía infantil, tiene como finalidad reforzar las medidas de protección de los menores, incluida su protección contra la explotación sexual, mediante la modernización de las disposiciones del derecho penal con el fin de circunscribir de manera más eficaz la utilización de los sistemas informáticos en relación con la comisión de delitos de índole sexual contra menores.

Esta disposición responde a la preocupación de los jefes de estado y de gobierno del Consejo de Europa, y es acorde con la tendencia internacional encaminada a lograr la prohibición de la pornografía infantil, como se evidencia del Protocolo Facultativo de la Convención de las Naciones Unidas sobre los Derechos del Niño relativo a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía, y por la iniciativa de la Comisión Europea relativa a la lucha contra la explotación sexual de los niños y la pornografía (COM2000/859).

Esta disposición establece como delitos diversos aspectos de la producción, posesión y distribución electrónica de pornografía infantil.

La mayoría de los estados ya han establecido como delito la producción tradicional y la distribución física de pornografía infantil. Con todo, debido al uso creciente de Internet como principal instrumento para el comercio de tales materiales, se consideró sin lugar a dudas que era esencial establecer disposiciones específicas en un instrumento jurídico internacional para combatir esta nueva forma de explotación sexual que representa un peligro para los menores.

La opinión generalizada es que los materiales y prácticas en línea, tales como el intercambio de ideas, fantasías y consejos entre los pedófilos, desempeñan un papel para apoyar, alentar o facilitar los delitos de índole sexual contra los menores.

El Informe Explicativo de la Convención de Budapest señala que la posesión de pornografía infantil estimula la demanda de dichos materiales. Una manera eficaz para reducir la producción de pornografía infantil es imponer consecuencias penales a la conducta de cada participante que intervienen en la cadena desde la producción hasta la posesión.

Asimismo, la directiva 2011/93/UE del Parlamento Europeo y del Consejo del 13/12/2011, relativa a la lucha contra los abusos sexuales y la explotación sexual de menores y la pornografía infantil ha condicionado y directamente inspirado la reforma que a nivel internacional han encarado los países respecto de los tipos de pornografía infantil.(2)

Hoy la Argentina se suscribió a la Convención de Budapest que, en su cuarto párrafo, permite a las partes hacer reservas respecto de la tenencia de material de pornografía infantil. Sin embargo, nuestro país ha dado un paso adelante con la sanción de la ley 27436.

III - ¿QUÉ ES MATERIAL DE PORNOGRAFÍA INFANTIL Y COMPORTAMIENTO SEXUALMENTE EXPLÍCITO?

Ante todo, es importante tomar conciencia del contenido que se prohíbe *tener*. Son fotografías y/o videos en los que bebés, niños y/o adolescentes aparecen siendo abusados sexualmente por una o más personas, o bien se encuentran posando en posiciones eróticas o sexuales, o realizando alguna actividad sexual.

La expresión "comportamiento sexualmente explícito" abarca por lo menos las siguientes alternativas: a) las relaciones sexuales, ya sea en forma genital-genital, oral-genital, anal-genital u oral-anal, entre menores o entre adulto y menor, del mismo sexo o del sexo opuesto; b) la bestialidad; c) la masturbación; d) los abusos sádicos y masoquistas en un contexto sexual, o e) la exhibición lasciva de los genitales o la zona pública de un menor.(3)

IV - ESCENARIO ACTUAL

El avance de la tecnología crea constantemente nuevas modalidades que corresponde analizar cuidadosamente si debieran ingresar al ámbito del derecho penal y, de introducirse, dilucidar si conforman conductas delictivas autónomas o pueden adaptarse a los tipos penales ya existentes.

En ese sentido, es indiscutible que el alcance e impacto de Internet y las redes sociales nos hace replantear el análisis del escenario delictivo, de sus autores y de las víctimas, pues el ciberespacio facilita la comisión de delitos y, en muchos casos, permite que se perpetúen en el tiempo a través de la viralización, indexación, distribución y facilitación del material delictivo.

La Fiscalía General de la Ciudad Autónoma de Buenos Aires firmó un Convenio con el *National Center for Missing and Expotation Children* (NCMEC), el día 11/10/2013.(4)

(2) LO 1/2015 - España - 30/3

(3) Informe explicativo Convención de Budapest - rm.coe.int

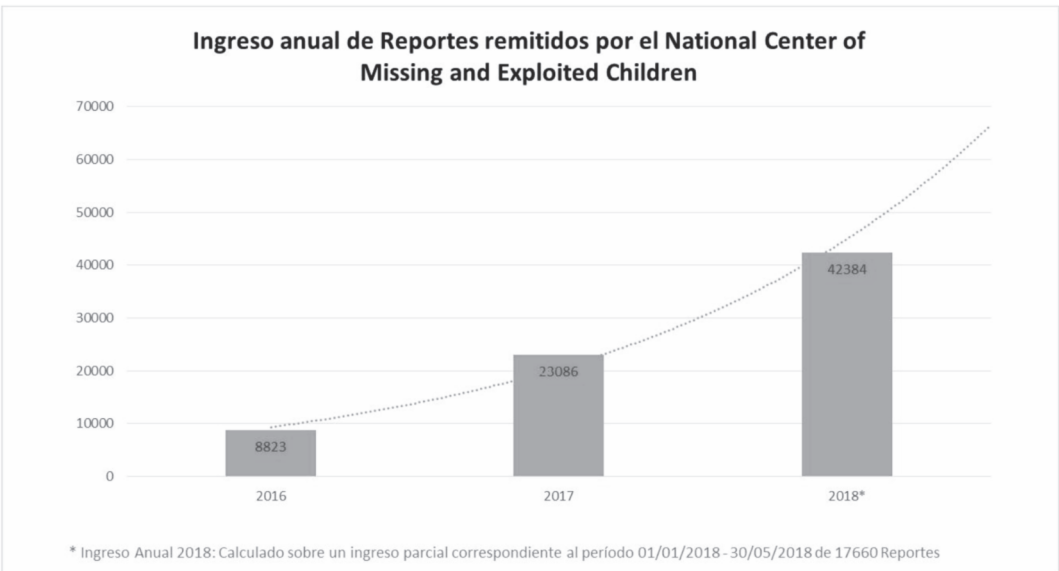
(4) R. (FG) 435/2013 - 12/11/2013

El NCMEC es una organización sin fines de lucro con sede en los Estados Unidos de América. Esta institución ha recibido apoyo del Congreso norteamericano 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 8.823 reportes y, en 2017, 23.086.



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, etc.-.

El resto ingresa para su correspondiente investigación y se pueden 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 detectaron 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.
5. Y además hay prueba -digital y/o física- de abuso sexual y/o corrupción de menores.

Ante cualquiera de estos posibles escenarios, y ante la imposibilidad de evitar analizarlos 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 diferente, 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* sin antes haber *abusado sexualmente de un niño.*

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 incluso más cantidad de material pornográfico con la intervención de menores.

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".*(5)

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.

En igual sentido, el fundamento político criminal que originó la aprobación de la criminalización de la posesión de material pornográfico infantil en Estados Unidos fue que dicha tenencia facilita la reproducción permanente e infinita de una situación concreta de abuso o agresión sexual, toda vez que lo que se observa en las imágenes es la vulneración de los derechos de uno o más niños. Por ende, el poseedor participa o contribuye con ese hecho al tomar parte de la cadena de mercado ya que la demanda por más material incentiva a los productores a cometer abusos.(6)

El ciclo de la pornografía infantil, desarrollada por el Dr. O'Brien en 1983 según Akdeniz(7), consiste en los siguientes pasos: a) la pornografía infantil se muestra a los niños con fines educativos, b) se intenta convencer a los niños que el sexo explícito es

(5) Fernández Teruelo. J.: "Cibercrimen. Aspectos de derecho penal y procesal penal. Cooperación internacional. Recolección de evidencia digital. Responsabilidad de los proveedores de servicios de internet", Dupuy. Daniela (Dir.) - Ed. BdeF. - Madrid - 2016 - pág. 63

(6) Schmidt-sandwick, Robin: "Constitutional law-freedom of speech: Supreme Court strikes down two provisions of the child pornography prevention act, leaving virtual child pornography virtually unregulated. Ashcroft v. Free Speech Coalition, 122 S. CT.1389 2002, North Dakota Law Review, t.79. 2003 - pág. 186

(7) Akdeniz, Yaman: "Internet Child Pornography and the Law: National and International Responses" - Padstow, Cornwall: TJ International ltd - 2008

aceptable, incluso deseable, c) el niño está convencido de que otros niños tienen una vida sexual activa y que tal conducta es correcta, d) la pornografía infantil desensibiliza al niño, reduce sus inhibiciones, e) algunas de estas sesiones progresarán con actividades sexuales que involucran al niño, f) se toman fotografías o videos de la actividad sexual, g) este nuevo material se distribuye en las redes internacionales de pornografía infantil y también, para atraer, seducir y obtener más víctimas menores.

A todo ello, se debe agregar las consecuencias: *el adquirente de pornografía infantil cada vez que pasa en video las imágenes reproducidas -a veces de menores de cinco o seis años de edad, e incluso de bebés-, perpetúa el ataque a la libertad y a la dignidad de los niños que han sido grabados previamente por si fuera poco el trauma sufrido por haber sido objeto de brutales agresiones sexuales filmadas o fotografiadas, que probablemente van a influir determinante y negativamente en el desarrollo adulto de su vida sexual y sentimental, encima se les quiere hacer soportar que los bienes jurídicos de su dignidad y de su intimidad, puedan seguir siendo pisoteados continuamente, sin consecuencia jurídica penal alguna, cada vez que un pedófilo decida contemplar las imágenes del atropello del que aquellos fueron objeto en la infancia".*[8]

V - POR QUÉ PENALIZAR LA TENENCIA DE PORNOGRAFÍA INFANTIL

La punibilidad de la mera posesión de los objetos prohibidos representa un adelantamiento de las barreras de protección mediante el castigo estatal de una etapa preparatoria, cuyo riesgo para el bien jurídico puede concretarse si se ejecutare un delito utilizando alguna de aquellas cosas no permitidas.

El creciente auge de esta categoría dogmática de delito se debe a la búsqueda de una mayor eficiencia del derecho penal de riesgo, siendo los delitos de posesión una herramienta útil para luchar contra la delincuencia.

Sin embargo, considero que es vital distinguir las diferentes problemáticas para evaluar concretamente la posibilidad de riesgo y así evitar que se cometan conductas más graves con consecuencias irreversibles.

En esta línea, y tal como lo expresara en otra oportunidad[9], no es lo mismo *tener* material de pornografía infantil que tener estupefacientes para consumo propio. Quien decide consumir drogas, afecta su propia salud; quien consume pornografía infantil, afecta la integridad sexual de los niños.

Gimbernart Ordeig así lo explica[10]: *"El bien jurídico protegido en los delitos de tráfico de drogas es la salud, y el titular de ese bien jurídico es el adquirente … y no se puede castigar la adquisición para el propio consumo de una sustancia que solo potencialmente puede menoscabar la vida o la salud de quien legítima y libremente puede disponer de ellas. En cambio, el bien jurídico protegido en un eventual delito de adquisición de pornografía infantil no pertenece al comprador, sino a un tercero (por ejemplo, al bebé cuya libertad e indemnidad sexual son brutalmente atropelladas por el productor pornográfico); por lo que al contrario de lo que sucede con quien se procura droga, el adquirente no tiene ninguna legitimación para disponer de los intereses de un tercero".*

(8) Gimbernat Ordeig, Enrique: "La teoría del bien jurídico" – Ed. Marcial Pons - Madrid - pág. 11 y ss.
(9) Fernandez Teruelo. J.: "Cibercrimen. Aspecto de Derecho penal y procesal penal", Dupuy. Daniela (Dir.) - Ed. BdeF. - Madrid - 2016 - pág. 123 y ss.
(10) Gimbernat Ordeig, E.: "Estado de derecho y ley penal" - LL - Madrid - 2009 - pág. 206 y ss.

En igual sentido, Fletcher[11] va más allá y señala que existe una diferencia de tratamiento en el delito de posesión de herramientas destinadas a cometer los delitos de robo o hurto, por ejemplo, frente a los cuestionamientos que se presentan al momento de decidir los casos vinculados a la posesión de material pornográfico infantil. Manifiesta que existen dos razones que justifican la diferencia de tratamiento sobre la base de distinguir entre "criminalidad manifiesta" *(manifiest criminality)* en contraste con la "criminalidad subjetiva" *(subjetive criminality).* En tal sentido, se debe diferenciar entre los delitos de posesión en donde solo el hecho de detentar la tenencia material de un objeto puede dar lugar a graves consecuencias materiales *(sinister implications)*, por el riesgo o peligro que representa ese hecho *per se,* como se desprende concretamente de la tenencia de material pornográfico infantil, en el que la experiencia enseña que generalmente son mantenidos con fines ilícitos; de los casos de tenencia de herramientas para la realización de los delitos de hurto o robo; en donde es exigible la acreditación del conocimiento de la prohibición del porte y la existencia de un fin diverso, pues precisamente la posesión de tales objetos no entraña inequívocamente un riesgo, porque no es dable pensar que se trata de elementos peligrosos para quienes tomen contacto con ellos.

Por lo expuesto, la posesión de cosas se la puede prohibir bajo amenaza de pena si se la asocia a un determinado fin delictivo, por parte del poseedor, que permita afirmar su carácter peligroso para algún bien jurídico.

En ese sentido, psiquiatras expertos en el tratamiento de quienes cometen este tipo de delitos contra menores de edad -pornografía infantil, *grooming*, abuso sexual, etc.- aseguran que la tenencia es un comienzo. Luego, y en razón de la lógica del funcionamiento de estas redes, dichos individuos son propensos a distribuir las imágenes sexuales que recibieron y son propensos a animarse a efectuar acercamientos a niños para abusar de ellos. No es casual que gran parte de ellos tienen un trabajo que les permite estar en contacto diario con los menores.

Concretamente, el fundamento para la criminalización de la tenencia de pornografía infantil se basa en el interés superior de la infancia, pues es la reproducción constante y la difusión de un abuso o agresión sexual cometida en contra de un niño que carece de la capacidad de autodeterminación en el ámbito sexual.

En ese sentido, el daño ya provocado a ese niño derivado del abuso sexual practicado durante la producción lo ha sido porque el poseedor tiene una responsabilidad en el comportamiento de quienes producen. Su conducta -*tener*- incentiva la producción y realización de otros abusos sexuales.

En este orden de ideas, entiendo que quienes almacenan en sus dispositivos informáticos imágenes de pornografía infantil para satisfacer sus deseos personales tienen probabilidad de agredir o abusar sexualmente de los niños; entonces, su tipificación operaría como una forma de control discrecional de la sociedad, entendiéndose como una manifestación de criminalidad objetiva, por cuanto la tenencia de material pornográfico infantil puede provocar graves riesgos y peligros.

En España, la tenencia de pornografía infantil va más allá con la reforma 1/2015: no solo es delito tener sino también adquirir o poseer material pornográfico virtual o técnico, lo cual amplía el radio de las conductas típicas relacionadas con la posesión.[12]

(11) Fletcher, G.: "Rethinking Criminal Law" - 2ª ed. - New York. Oxford University Press - 2000, nota 52 - pág. 200 cit. Oxman, Nicolás en: "Aspectos políticos-criminales y criminológicos de la posesión de pornografía infantil en EE. UU." - Política Criminal - Nº 12 - 2011, art.2. - vol. 6 - págs. 253-295

(12) Circular 2/2015 de la Fiscalía General del Estado de España sobre los delitos de pornografía infantil operado por LO 1/2015. En: fiscal.es

VI - UN PASO MÁS

Ya es ley la tenencia. Es necesario dar un paso más.

En primer lugar, pronostico un considerable aumento de casos a investigar que antes eran apartados tempranamente por atipicidad.

Hoy, si los hechos fueron cometidos con posterioridad a la sanción de la ley, ingresarán al universo diario de investigaciones.

Considero fundamental efectuar una gestión eficiente de los nuevos casos, efectuando su tratamiento especial y superador con miras a la prevención, a la profunda concientización de las consecuencias que este accionar genera.

En primer lugar, analizar cada caso en particular para poder distinguir -y comprobar- quiénes tienen el material de pornografía infantil con fines inocentes, o con desconocimiento de tal posesión, de aquellos otros que lo poseen porque forman parte del círculo estudiado. Dicha circunstancia será analizada en el contexto del plexo probatorio en cada caso concreto.

Una vez descartada la posibilidad de error, y toda duda sobre su autoría, es importante adoptar decisiones de calidad en relación con los autores de la tenencia, a fin de implementar, con la intervención de psicólogos y psiquiatras expertos en perfiles de personalidad perversa, un programa de tratamiento y concientización de la implicancia de estas conductas, con el fin de evitar reincidencias, conductas más graves y, por sobre todo, el aumento escandaloso de víctimas menores de edad.

Entiendo que sería innovador crear y aplicar -como prueba piloto y por un tiempo establecido- un protocolo de actuación con intervención multidisciplinaria para, luego de ese lapso temporal, evaluar su impacto en la probable disminución de la comisión de estas modalidades directamente conectados con la lesión a la integridad sexual de los niños.

El diagnóstico ya existe. Debemos trabajar a conciencia con las personas que consumen el material prohibido pues la tenencia representa la línea de largada, el comienzo de un camino que deja huellas irreversibles en la vida de los niños.

VII - CONCLUSIÓN

Considero que la sanción de esta ley fue un gran avance pues se tuvo en cuenta la opinión de los investigadores, quienes a diario sentíamos la impotencia de conocer a fondo la problemática y las consecuencias de la implicancia del *tener* y no poder aplicar la ley pues no existía.

Los legisladores comprendieron a la perfección la dinámica de la tenencia y del círculo de la pornografía infantil, y votaron en consecuencia -211 votos a favor y solo una abstención-, sancionando la ley.

El alcance de esta nueva legislación es aún mayor: la posibilidad de cooperación internacional recíproca entre todos los países en los que la tenencia es delito.

Es cierto que estábamos ante una importante disyuntiva, ambas de peso: la racionalidad de las demandas de la sociedad de mayor seguridad frente a la posible tensión de los delitos de tenencia con los principios constitucionales del derecho penal sustantivo -derecho a la privacidad e intimidad, entre otros-.

La comunidad ha optado por mayores cuotas de seguridad en desmedro de las libertades. Y en ese sentido se expide Cox Leixelard(13), al expresar que no es posible inferir que la pretensión de eficiencia penal implica el abandono de un modelo de garantías. Por el contrario, la expansión del derecho penal a través del aumento de las incriminaciones de las figuras de posesión se desarrolló tomando como base principios tradicionalmente considerados garantísticos. De hecho, los principios del daño y de exclusiva protección de bienes jurídicos frente al poder del Estado sirven hoy para aumentar el castigo y relajar las garantías.

Y el efectivo análisis de la realidad empírica extraída de los casos que ingresan creciente e incesantemente al ámbito penal, y su lógica encadenada a un círculo perfecto que termina -o comienza- en el abuso sexual de niños/as, demanda su efectiva y correcta tipificación.

El desafío no termina en que la tenencia sea ley. Ello es tan solo el comienzo de un proceso en el que debemos trabajar a conciencia y profesionalmente para un abordaje efectivo, y eso hace imprescindible fijar pautas hermenéuticas para alcanzar una respuesta uniforme y respetuosa con los principio de igualdad ante la ley, seguridad jurídica, proporcionalidad y culpabilidad, con el fin de evitar que se comentan delitos de la especie más graves y desalentar así la posesión del material que, inexorablemente, para poder *tenerlo*, previamente hay que *abusar* de un niño.

(13) Cox Leixelard. J.P: "Delitos de posesión. Base para una dogmática" - Ed. B de F - 2012 - págs. 13 y ss.

La previsión normativa del tipo penal de *grooming* en la Argentina

Lucas Grenni(*)
Rodrigo Fernández Ríos(**)

I - INTRODUCCIÓN

Desde los inicios de internet en la década de 1960 hasta ahora ha sido exponencial el crecimiento y la masificación del acceso a la red. Sobre todo con el desarrollo de la World Wide Web, que en los últimos 20 años ha multiplicado el acceso a los usuarios en el hemisferio occidental.

Esta evolución ha tomado mayor velocidad a partir de la irrupción de las redes sociales, fenómeno que permitió que personas de diferentes lugares, sin importar la distancia, tengan contacto entre sí, pero también puso en situación de mayor vulnerabilidad a aquellos que no toman los recaudos suficientes a la hora de compartir su información. Estos avances se complementaron y amplificaron con la llegada de los dispositivos portátiles, *tablets*, *smartphones* y nuevas redes sociales.

Se destaca como sector vulnerable el de los niños, quienes anteriormente veían mucho más limitado su uso cuando accedían utilizando una computadora en su hogar, dado que el hecho de compartir el punto de acceso con su familia les permitía a los padres un mayor control respecto de las páginas que visitaban e incluso respecto de quienes formaban parte de las listas de contactos.

(*) Abogado (UBA). Especialista en Derecho Penal (USAL). Posgraduado de las universidades de Palermo, del Litoral y UBA. Corredactor del Código Procesal Penal de la Provincia de Jujuy. Profesor asociado de la materia Derecho Penal, Parte general (Universidad Católica de Santiago del Estero)
(**) Abogado (Universidad Católica de Santiago del Estero). Especialista en Derecho Penal (USAL). Doctorando en Derecho Penal y Ciencias Penales (USAL). Analista programador (Universidad Nacional de Jujuy)

Las *tablets* y *smartphones* trajeron consigo el acceso a las redes sociales durante las veinticuatro horas, casi ilimitado y con un control parental muy limitado, lo que hace que el ciberespacio sea cada vez más atractivo como terreno fértil para la comisión de delitos contra los niños. Ante esto ha surgido un movimiento político criminal tendiente a buscar la punición de las diversas conductas que lesionan bienes jurídicos mediante la utilización de la red, lo que ha llevado al surgimiento de nuevos tipos penales, entre los cuales se destaca en el último tiempo la tipificación del *grooming* en el derecho positivo argentino.

En relación con los tipos penales que forman parte de lo que se conoce como ciberdelito, cabe hacer una distinción previa entre aquellos tipos penales que surgen acompañados de nuevos objetos de tutela y aquellos que procuran evitar la afectación de un bien jurídico que ya se encuentra protegido por el derecho positivo, mediante nuevas modalidades surgidas de la utilización de medios informáticos.(1)

Con la promulgación de la ley 26904, se incorpora al Código Penal (CP) argentino un nuevo tipo penal que se denomina internacionalmente con el nombre de "*grooming*" o "*childgrooming*". Este tipo penal está orientado a la protección de la integridad sexual de los menores que acceden a internet. En la redacción argentina se tomó como modelo aquel instaurado en el código penal español y ha sido un sincero intento de adecuar la legislación a las exigencias que surgen del Convenio sobre Cibercriminalidad de Budapest.

La conducta en cuestión tiene como consecuencias tanto la difusión de imágenes de pornografía infantil como abusos sexuales a menores de edad. Sin embargo, la forma en que ha sido legislada plantea diversas consideraciones, no siendo la menor de ellas el debate respecto de su constitucionalidad, ya que hay sectores que resaltan, no sin razón, el carácter de acto preparatorio que tiene la conducta descripta por el tipo penal.

Se debe poner énfasis también en todos los inconvenientes que se derivan de la difícil actividad probatoria que requiere este tipo de delito, la velocidad de cambio de los dispositivos electrónicos y protocolos de comunicación e intercambio de datos, pero sobre todo de las diferentes técnicas que constantemente desarrollan los cibercriminales, que normalmente van por delante de las estrategias de defensa desarrolladas por los especialistas.

Otro problema que surge con la tipificación de los delitos informáticos -y no menor, por cierto- es que las leyes penales están normalmente pensadas para ser aplicadas en un Estado determinado, y este tipo de delitos en la mayoría de las ocasiones trasciende las fronteras nacionales e incluso puede llegar a tomar dimensiones globales(2). Esta situación obliga al legislador a procurar adoptar, armonizar y unificar criterios surgidos de las diferentes legislaciones internacionales a los fines de reducir al máximo el margen de impunidad para este tipo de conductas.

Se ha fundado la necesidad de tipificar esta conducta argumentando que se trata de una decisión de política criminal necesaria, ya que con el avance de las tecnologías y

(1) Cugat Mauri, Miriam: "La tutela penal de los menores ante el *online grooming*: entre la necesidad y el exceso" en Riquert, Marcelo A. (Coord.): "Ciberdelitos. *Grooming. Stalking. Bullyng. Sexting.* Ciberodio. Propiedad intelectual. Problemas de perseguibilidad. Ciberpornografía infantil" - Ed. Hammurabi - Bs. As. - 2014 - pág. 253

(2) Riquert, Marcelo A.: "Repensando cómo funciona la ley penal en el ciberespacio" en "Ciberdelitos. *Grooming. Stalking. Bullyng. Sexting.* Ciberodio. Propiedad intelectual. Problemas de perseguibilidad. Ciberpornografía infantil" - Ed. Hammurabi - Bs. As. - 2014 - pág. 17

la masificación de los medios electrónicos los pedófilos y pederastas, en lugar de buscar sus víctimas en plazas, parques o jardines de infantes han encontrado un terreno fértil sobre todo a través de las redes sociales, medio que les permite contactar a sus víctimas con un riesgo mínimo.(3)

El objetivo de este trabajo es detectar y analizar los problemas que surgen a partir de la sanción de este tipo penal, las diferentes formas en que ha sido legislado en el derecho internacional y su adecuación a la teoría del delito, pero, principalmente, su constitucionalidad y el respeto de los principios limitadores de la pretensión punitiva estatal.

II - EL CONCEPTO DE "DELITO INFORMÁTICO"

a) Antecedentes

En primer lugar, antes de adentrarnos específicamente en el delito de *grooming*, corresponde analizar brevemente lo que se entiende conceptualmente como delito informático.

El concepto de delincuencia relacionada con computadoras aparece por primera vez en los Estados Unidos a finales de la década del sesenta, principalmente en artículos periodísticos.(4)

Posteriormente, durante los años setenta nace el movimiento reformista respecto de la normativa relacionada con la recolección, almacenamiento y transmisión de datos personales en computadoras y redes informáticas, y es el primer abordaje realizado desde el punto de vista legal relacionado con la criminalidad informática el estudio desarrollado por el jurista alemán Ulrich Sieber en 1977.

En 1979 surge del *Stanford Research International Institute* la primera definición realizada sobre delitos informáticos, a pedido del Departamento de Justicia de los Estados Unidos, según la cual se consideraba delito informático a "*cualquier acto ilegal donde el conocimiento de la tecnología computacional es esencial para el éxito de su prosecución*"(5). Como se observa, esta primera definición pone el énfasis no en la conducta en sí desplegada por el sujeto activo sino en los conocimientos necesarios para la prosecución del delito.

Luego, en 1983 fueron definidos por la Organización de Cooperación y Desarrollo Económico (OCDE) como "*cualquier comportamiento antijurídico, no ético o autorizado, relacionado con el procesamiento automático de datos y/o transmisiones de datos*". Nótese que, si bien no se trata de una definición demasiado precisa, mejora a la anterior debido a que pone el prisma sobre el comportamiento del autor, en lugar de definirlo por los conocimientos requeridos para lograr la punición de la conducta.

(3) Buompadre, Jorge: "*Grooming*" - Publicado en la Página web de la Asociación Pensamiento Penal. Ver en: pensamientopenal.com.ar

(4) Sain, Gustavo: "¿Qué son los delitos informáticos?" - Ed. Rubinzal-Culzoni online - RC D 875/2015

(5) Conf. Sain, Gustavo: "¿Qué son los delitos informáticos?" - Ed. Rubinzal-Culzoni online - RC D 875/2015

Por otro lado, el Consejo de Europa en el año 2001 gestó el convenio que en la actualidad resulta el marco de referencia en lo relacionado a la ciberdelincuencia, el Convenio sobre Cibercriminalidad de Budapest. De acuerdo con este instrumento, los delitos informáticos se clasifican en cuatro categorías, a saber:

a) delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos;
b) delitos informáticos propiamente dichos, falsificación y estafa informática;
c) delitos relacionados con contenidos; y
d) violaciones a la ley de propiedad intelectual.

Existen otras clasificaciones también desde el criterio legal, que entiende que las conductas en cuestión podrán considerarse delito cuando se encuentren penadas por la ley o cuando sean susceptibles de tipificación.(6)

En el año 2002, el Consejo de la Unión Europea brindó una definición que tampoco resulta muy esclarecedora al respecto, dado que los entiende como "*cualquier delito que de una forma u otra implica el uso de tecnología de la información*".(7)

Como se observa, las definiciones resultan bastante imprecisas y dispares; esto sucede, de acuerdo a lo expresado por el criminólogo Majid Yar, debido a que "*…la delincuencia informática se refiere no tanto a un único tipo de actividad delictiva, sino más bien a una amplia gama de actividades ilegales e ilícitas que comparten en común el único medio electrónico (ciberespacio) en el que tiene lugar*"(8). El aporte de esta definición radica en resaltar el medio en el cual se comete el delito, internet, como el medio electrónico por excelencia para cometer delitos de esta categoría.

Es que también debemos distinguir entre aquellos delitos que se consideran informáticos por los elementos o los medios utilizados para su comisión pero que involucran conductas que ya se encuentran penadas dentro de nuestra legislación. Por ejemplo, las estafas realizadas utilizando teléfonos móviles, que son delitos que involucran conductas novedosas que no se encontraban alcanzadas por tipos penales existentes con anterioridad. Otro caso podría ser el daño de un sistema informático a través de la utilización de un virus.

A veces, al clasificar los delitos informáticos se pone el acento en el hecho de que los dispositivos informáticos son utilizados como un simple medio para cometer un delito o que estos sean el blanco del ataque propiamente dicho.

De lo anteriormente explicado vemos que resulta cuanto menos difícil armonizar una definición de delito informático. Sin embargo, a partir de la firma del Convenio de Budapest podemos decir que existe una suerte de movimiento político criminal internacional orientado a punir los delitos que se realizan utilizando medios informáticos tanto como aquellos que se realizan teniendo como blanco sistemas y dispositivos informáticos.

Otro mito en relación con los delitos informáticos que debe derrumbarse es el hecho de que estos solo pueden ser cometidos por *hackers* o que requieren niveles avanzados de conocimiento informático para ser realizados. En la actualidad, debido a la masividad del

(6) Sain, Gustavo: "¿Qué son los delitos informáticos?" - Ed. Rubinzal-Culzoni online - RC D 875/2015

(7) Conf. Sain, Gustavo: "¿Qué son los delitos informáticos?" - Ed. Rubinzal-Culzoni online - RC D 875/2015

(8) Yar, Majid: "Cybercrime and Society" - Sage Publications Ltd. - 2006

acceso a internet, cualquier persona con una computadora puede tomar contacto con tutoriales y herramientas que permiten desde aprender a falsificar un correo electrónico hasta ingresar a sistemas protegidos, sea para robar información o causar daños.Pero eso no es todo, tomemos el caso de quienes distribuyen pornografía infantil como ejemplo: muchas veces se interiorizan sobre la existencia de herramientas de cifrado de información o servicios de correo electrónico que permiten el envío de mensajes cifrados y se valen de ellos para, sin mayores conocimientos de informática, distribuir este tipo de material.

Otro ejemplo de esto es que en el año 2014 el delito relacionado con la informática más denunciado ante el Centro de denuncias de Crímenes por Internet del FBI fue el fraude en la venta de vehículos. La mecánica radica en ofrecer un automóvil en una red social o en una página web, generalmente a un precio muy bajo, consiguiendo que la víctima transfiera una cantidad de dinero en concepto de adelanto(9); como vemos, esto no requiere grandes conocimientos de informática de parte del autor del delito.

Finalmente, debemos resaltar que, además de resultar difíciles de definir, también resulta complejo para el sistema penal investigar y punir estas conductas, porque el ciberdelito evoluciona rápidamente y surgen nuevas técnicas prácticamente a diario. Resultan entonces difíciles de detectar e investigar con los métodos tradicionales de investigación, sobre todo porque su prevención y control demandan que los agentes del sistema penal desarrollen competencias y habilidades similares a las de los ciberdelincuentes.(10)

b) Propuesta de delimitación conceptual de delito informático

Siguiendo a Anzit Guerrero, Tato y Profumo, la doctrina argentina define al delito informático como: "*toda acción (acción u omisión) culpable realizada por un ser humano, tipificado por la ley, que se realiza en el entorno informático, y está sancionado con una pena*".(11)

Será entonces toda aquella acción antijurídica y culpable, que se da por vías informáticas o que tiene como objetivo destruir y dañar ordenadores, medios electrónicos y redes de internet. La criminalidad informática consiste en la realización de un tipo de actividades que, reuniendo los requisitos que delimitan el concepto de delito, sean llevados a cabo utilizando un elemento informático.(12)

Haciendo un análisis desde la teoría del delito, podríamos decir entonces que el delito informático es una conducta típica, antijurídica y culpable, que se realiza utilizando dispositivos informáticos como medio -con dispositivos o sistemas informáticos como blanco-, que pueden cometerse a través de internet y que pueden ser cometidos por cualquier individuo.

(9) Federal Bureau of Investigation: "Internet Crime Complaint Center" - 2014 Internet Crime Report - Ver en: ic3.gov

(10) Siegel, Larry J.: "Criminology" - 11a ed. - Wadsworth Cengage, Learning - Belmont - USA - 2012 - pág. 520

(11) Anzit Guerrero, Ramiro; Tato, Nicolás S. y Profumo, Santiago: "El derecho informático - Aspectos fundamentales" - Ed. Cátedra Jurídica - Bs. As. - 2010 - págs. 145/6

(12) Correa, Carlos; Batto, Hilda; Czar de Zalduendo, Susana y Nazar Espeche, Félix: "El derecho ante el desafío de la informática" en "Derecho informático" – Ed. Depalma – Bs. As. - 1987 - pág. 295. Cuervo, José: "Delitos informáticos: protección penal de la intimidad" - informatica-juridica.com - 2008

III - EL *GROOMING*

a) Concepto

Como hemos mencionado anteriormente, el acceso casi irrestricto a internet y a las diferentes redes sociales, entre otras *facebook, snapchat* y *twitter*, permite que el usuario se exponga al mundo; esto atrae a personas sin malas intenciones, pero también atrae a algunas que se encuentran motivadas para cometer diversos delitos.

Entre los distintos delitos que se cometen valiéndose de internet, de acuerdo a estimaciones realizadas por el FBI, los principales son aquellos que tienen contenido patrimonial, seguidos muy de cerca por los delitos sexuales. Entre estos últimos los más comunes son la difusión de pornografía infantil y el *grooming*, ambos íntimamente relacionados.

Cuando hablamos de *grooming*, hacemos referencia, de acuerdo con la definición de Vaninetti, a "… *todas las prácticas desplegadas en línea por ciertos adultos, pederastas y pedófilos, conocidos en la red como 'groomer', para ganarse la confianza de un menor fingiendo empatía, cariño, etc. normalmente bajo una falsa identidad de otro menor, con la finalidad de satisfacer sus apetencias sexuales*".(13)

De acuerdo con el manual "DSM" de la "*Asociación Estadounidense de Psiquiatría*", la pedofilia es una parafilia en la cual la persona siente un intenso y recurrente deseo y fantasías sexuales hacia niños o niñas que aún no han llegado a la adolescencia. En cambio, la pederastia es cometer un abuso sexual de un menor.(14)

Se colige de lo dicho que el *grooming* puede tener como autores a aquellos que tienen como fin concretar un abuso sexual tanto como aquellos que desean inducir a menores a tomarse fotografías con contenido erótico.

Puede tentarse como definición del delito de *grooming* el despliegue de técnicas y estrategias, por parte de un mayor de edad, valiéndose de la red telefónica, internet y dispositivos electrónicos, con la finalidad de ganar la confianza de menores para obtener información personal e incluso en algunos casos imágenes de contenido sexual, aunque sin que esto último sea un requisito necesario, que permitan extorsionar a la víctima, sea para la obtención de imágenes con mayor contenido explícito o para concretar un encuentro sexual.

b) Naturaleza del *grooming*

En relación con la naturaleza del *grooming* existen diferentes posturas doctrinarias. Existen aquellos que, dentro de un sector minoritario, sostienen que es una figura criminológica, compuesta de un abanico más o menos acotado de conductas realizadas por un sujeto contra un menor de edad.(15)

(13) Vaninetti, Hugo A: "Inclusión del '*grooming*' en el Código Penal" - LL - 16/12/2013 - pág. 1 - LL2013-F, 1200 - LLP 2014 (marzo)

(14) American Psychiatric Association: "Manual diagnóstico y estadístico de los trastornos mentales" - 5ª ed. - 2013 - DSM-V

(15) Anderson, Wade: "Criminalizing virtual child pornography under the child pornography prevention act: is it really what it appears to be?" - Ed. University of Richmond Law Review - 2001 - pág. 396

Existe otro grupo que entiende que el delito de *grooming* criminaliza los actos preparatorios tendientes a la concreción de otro delito que lesiona la integridad o libertad sexual de una persona menor de edad.(16)

En la doctrina argentina, Buompadre también se ha manifestado en concordancia con esta teoría, entendiendo que la voluntad del legislador ha sido adelantar barreras de protección incriminando conductas que se caracterizan como actos preparatorios de los delitos sexuales contenidos en nuestro CP.(17)

Respecto a lo expresado por esta última postura es que se encuentra muy criticado el tipo penal, dado que nuestro derecho positivo considera que los actos preparatorios no son punibles, salvo que haya existido un comienzo de ejecución dando lugar a la aplicación de las reglas de la tentativa.

c) Diferenciación del *grooming* de otras figuras penales

Es importante diferenciar el *child grooming* -o simplemente *grooming*- de la conducta extorsiva que puede producirse para la obtención de imágenes o información utilizando otros medios (por ejemplo, el robo de contraseñas, ingeniería social, sustracción de dispositivos, etc.). En estos casos nos encontraríamos ante conductas punibles de diferente naturaleza que la del *grooming*, por lo que podrían encuadrar en distintos tipos penales de conformidad a la legislación vigente.

Tampoco se considera *grooming* la conducta desplegada por un adulto que contacta por medios informáticos a un menor pero que no tiene otra finalidad que el contacto mismo, aunque puedan existir conversaciones con contenidos sexuales entre ellos. Otras conductas que no se considerarán como comprendidas por este delito serán las desplegadas por un adulto que contacte a otro adulto, aunque el sujeto activo tenga como finalidad cometer un delito de naturaleza sexual.

d) Mecanismo comisivo

Al analizar la conducta propiamente dicha, vemos que incluye a todas aquellas técnicas que permitan ganar la confianza del menor a través de internet; dentro de estas técnicas podemos destacar la creación de perfiles falsos, la sustitución de identidad, el uso del chat e incluso de mensajes de texto.

La actividad del adulto normalmente inicia con la creación de un perfil falso o el ingreso con el de otro menor a una red social, aunque también puede utilizar mensajes de texto a través de *smartphones* o *tablets* para tratar de contactar a menores. Una vez iniciado el contacto, comienza a mantener conversaciones a través de la red, cada vez con mayor frecuencia, hasta ganar su confianza; luego de haber recabado suficiente información sobre la vida privada del menor, trata de convencerlo de intercambiar imágenes o mensajes con contenido sexual.

(16) Cugat Mauri, Miriam: "La tutela penal de los menores ante el *online grooming*: entre la necesidad y el exceso" en Riquert, Marcelo A. (Coord.): "Ciberdelitos. *Grooming. Stalking. Bullyng. Sexting.* Ciberodio. Propiedad intelectual. Problemas de perseguibilidad. Ciberpornografía infantil" - Ed. Hammurabi - Bs. As. - 2014 - pág. 275

(17) Buompadre, Jorge: "El grooming" - Publicado en la Página web de la Asociación Pensamiento Penal. Ver en: pensamientopenal.com.ar

Estas fases no tienen una duración determinada, varían de acuerdo a la habilidad del adulto para ganarse la confianza y la mayor o menor precaución que el menor tenga para relacionarse con extraños y proteger su información personal.

Lo primero que debemos mencionar es que resulta fundamental que el medio elegido para contactar al menor haya sido uno de los que se agrupa como parte de las tecnologías de la información y la comunicación (TIC), como teléfono, internet, etc.

Normalmente el pedófilo ingresa en una red social o canal de chat público con un perfil que en la mayoría de los casos no delata su verdadera edad, hace referencia a cosas populares entre niños o adolescentes, y trata de contactar a menores valiéndose de diferentes estrategias.

Es común que el *groomer* mienta no solo respecto de su edad, sino también en relación con su identidad sexual, hábitos, situación económica, etc.

Debemos destacar que, lejos de complicarse, el contacto en las redes sociales es cada vez más fácil debido a que existen redes como *Instagram* o *Twitter*, que se encuentran en el auge de popularidad y permiten que cualquiera, aunque no forme parte de nuestros contactos, pueda ver lo que publicamos. Además, otras redes sociales, como *Facebook*, permiten controlar quiénes tienen acceso a nuestras publicaciones, pero tratan de fomentar que hagamos cada vez más públicas nuestras actividades, facilitando enormemente esto. Recordemos que en un principio solo admitía que se compartieran únicamente fotos, pero en la actualidad permite incluso transmisión de videos en vivo, en tiempo real.

Esto permite a pedófilos conocer y tener una idea bastante precisa de los gustos, preferencias y actividades de sus potenciales víctimas aun antes de iniciar el contacto, brindándoles la posibilidad de diseñar estrategias más efectivas en aras de ganarse su confianza.

No es un detalle menor tampoco la poca educación que se brinda a la población en general sobre estrategias para resguardar la privacidad en Internet. En general, los textos sobre ciberseguridad están orientados a personas que ya tienen conocimientos previos del tema o que se dedican activamente a la administración de sistemas, por lo que no resultan accesibles para los usuarios comunes.[18]

Es así que, fingiendo compartir gustos, actividades o pertenencia a grupos sociales cercanos, el sujeto activo busca iniciar un contacto. Al principio, por lo general, lo hará de manera esporádica, buscando evitar las sospechas de parte de su víctima. Luego lo hará más frecuentemente, tratando de despertar su interés.

Durante esta etapa las conversaciones no incluyen temas sexuales, sino que más bien se limitan a cuestiones triviales. Al mismo tiempo el *groomer* va sondeando al menor para ver hasta qué punto puede responder favorablemente a sus propuestas, en general busca indicios como una baja autoestima, problemas con los padres, etc.

Cuando ya se ha ganado la confianza, comienza un verdadero juego de seducción mediante halagos, promesas de viajes, en definitiva, utiliza cualquier cosa que sea del gusto de la víctima. En muchos casos el pedófilo trata de entablar una relación cada vez más estrecha con la víctima valiéndose de regalos, uno de los más comunes son los teléfonos celulares, lo que permite que se comuniquen por una vía de la cual los padres de la víctima no están al tanto.

(18) Waschke, Marvin: "Personal cybersecurity. How to avoid and recover from cybercrime" - Ed. Apress - Washington - 2017 - pág. 13

Si tiene éxito en instaurar la temática sexual en las charlas, posteriormente buscará conseguir que el menor le envíe fotos de él o ella en ropa interior, sin ropa o exhibiendo sus genitales, pudiendo llegar a solicitar videos o fotos realizando prácticas sexuales como la masturbación.

Posteriormente logra que el menor inicie con él un intercambio de este tipo de material; se dice que allí es donde concluye la primera etapa. A partir de aquí el adulto toma el control de la situación, ya que, valiéndose de amenazas de difundir las imágenes que posee por la red o mostrárselas a los contactos del menor, comienza a extorsionarlo. Cabe aclarar que en muchos casos no existen elementos para una extorsión, pero el acosador, con su pericia, consigue convencer de su existencia a la víctima, la que accede a sus peticiones por temor.(19)

Luego de esa etapa normalmente el *groomer* revela su verdadera identidad, amenazando con que enviará esas imágenes a los padres, familiares o contactos del menor si no accede a sus demandas: es aquí que da inicio el acoso propiamente dicho(20). Este acoso puede limitarse a seguir solicitando material pornográfico del menor, o puede encontrarse direccionado a tratar de concretar un encuentro con la finalidad de cometer un delito de contenido sexual contra la víctima.

Es a partir de ese momento que, si la víctima responde de forma positiva, en primer lugar tratará de que la comunicación deje de ser por canales masivos o públicos, y buscará que los contactos se den en canales privados, por ejemplo por *Whatsapp* o servicios de e-mail. Una vez que el menor accede a comunicarse de manera privada, trata de llevar la conversación a temas de contenido sexual, cada vez más explícitos, observando la respuesta de la víctima a medida que suben de tono las conversaciones.

Hay que destacar que esto lo realizará de manera paulatina, con la finalidad de evitar que la víctima se asuste, buscando como resultado de esta modalidad operatoria que el menor se sienta cada vez más cómodo con estos temas.

e) Metodologías frecuentes de investigación

Debido a la particular situación en la de que el pedófilo busca eventualmente concretar con el menor un encuentro cara a cara, la investigación de los delitos de esta naturaleza resulta en muchos casos exitosa dado que las autoridades, en caso de tomar conocimiento de la reunión programada, están en condiciones de identificar y detener al autor.

Una modalidad muy utilizada para la investigación y prevención de este delito consiste en que un adulto, normalmente un miembro de las fuerzas de seguridad, se haga pasar por un menor.(21)

Esta metodología tan utilizada por el sistema penal de los Estados Unidos resulta muy controvertida en el marco de nuestro derecho positivo dada la dificultad de determinar hasta qué punto el adulto, actuando como un menor, no se convierte en un verdadero agente inductor de la conducta del autor. Al igual que otras formas de investigación utilizadas en el sistema anglosajón, como por ejemplo el agente encubierto, resultan discutibles desde el punto de vista constitucional.

(19) Ver en: internet-grooming.net

(20) Buompadre, Jorge: "El *grooming*" - Asociación Pensamiento Penal - Ver en: pensamientopenal.com.ar

(21) Easttom, Chuck: "Computer security fundamentals" - Ed. Pearson Education - Indianapolis - USA - 2016 - pág. 71

Asimismo, también presenta el problema de ser un delito imposible en el sentido de que carece de uno de los elementos del tipo penal objetivo, es decir, el sujeto pasivo, ya que el autor cree que habla con un menor pero en realidad lo está haciendo con un adulto. De tal suerte no habría real afectación del bien jurídico, y punir esa conducta por su inmoralidad o vocación delictiva implica incurrir en un derecho penal simbólico, o en su caso derecho penal de autor.

Otra técnica de prevención utilizada por algunos Estados de Estados Unidos consiste en publicar bases de datos *online* de "delincuentes sexuales" que permiten que cualquier persona consulte en ellas, a los fines de saber si la persona que se contacta con ellos por cualquier medio se encuentra o no dentro de esta categoría.

La posibilidad de implementar un verdadero derecho penal de autor que este tipo de lista representa resulta contraria a nuestro derecho y al sistema penal de nuestro país. Sin embargo, constantemente existen quienes abogan por la inclusión de este tipo de prácticas, sin reparar en la contradicción que representaría la vigencia de ellas en relación con nuestro derecho constitucional.

En nuestro país, lo más frecuente en la investigación de este tipo de delitos es la identificación y rastreo a partir de la dirección de IP utilizada para enviar los mensajes, siempre con la colaboración de los diferentes proveedores de servicio de internet, para determinar quién es el titular del servicio y demás datos que permitan determinar el posible autor.

En relación con esto podemos decir que la utilidad de la técnica será relativa, atendiendo a que para dificultar la labor de los investigadores bastaría con que el *groomer* se conecte desde diferentes lugares, algo sencillo dada la proliferación de las conexiones *wifi* públicas en nuestro país y la portabilidad de dispositivos como *tablets* o *smartphones*.

IV - EL TIPO PENAL DE *GROOMING* EN EL DERECHO ARGENTINO

a) Recepción normativa. Análisis de la previsión típica

En el año 2013, con la sanción de la ley 26904, se incorporó el *grooming* al CP. De acuerdo al texto de esta ley el tipo penal ha quedado definido en el artículo 131 de la siguiente manera: "*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*".

En primer lugar, advertimos de la lectura del artículo que la definición de la acción típica omite distinguir en el caso del autor entre mayores y menores, es decir que con esta redacción el autor puede ser tanto un mayor como un menor de edad.

Esto es contrario a lo que se entiende por *grooming*, debido a que, como se ha dicho, presupone que quien contacta al menor es un mayor de edad.

También se observa que los requisitos de acuerdo a nuestra legislación son el contacto con un menor, realizado por cualquier medio de comunicación y transmisión de datos, y que este contacto deberá ser con el propósito de cometer un delito contra la integridad sexual de la víctima.

Otra particularidad que encontramos respecto de la definición del *grooming* en nuestro derecho positivo es que se ha incluido a cualquier medio de comunicación y transmisión de datos, en un intento por evitar que el concepto caiga en desuso ante el avance tecnológico. Esto ha sido visto favorablemente por la doctrina: autores como Vaninetti, Tazza y Grisetti se han expresado a favor de este tipo más inclusivo en relación con otras legislaciones.(22)

Es requisito indispensable que el contacto haya sido realizado por medios de telecomunicación, es decir que se haya dado en un entorno virtual. Si se diera en el mundo real, no se configuraría la acción típica; en todo caso podríamos estar ante una tentativa o un acto preparatorio impune.(23)

Como se ve, estamos ante la punición de un acto preparatorio de otro delito, por lo que necesariamente el análisis de tipicidad de la conducta se debe completar con la intención de cometer un delito contra la integridad sexual de la víctima, es decir, debe dilucidarse la existencia de una intención, algo que resulta cuanto menos de muy difícil probanza, por no decir casi imposible.

Esto también torna difícil su aplicación y motiva objeciones sobre su constitucionalidad. Admitir que pueda ser punible una intención deviene en una espada de doble filo, dado que el día de mañana se podría con este criterio determinar que corresponde penar a quien tenga la intención de cometer un homicidio o lesiones respecto de un tercero. Sería ilógico si tenemos en cuenta que en un momento de enojo todos, en mayor o menor medida, hemos tenido alguna vez deseos de golpear a alguien en medio de una discusión acalorada.

En este sentido, como destaca Vaninetti, es más acertado el precedente extranjero obrante en el Convenio del Consejo de Europa para la protección de los niños contra la explotación sexual y el abuso sexual, dado que estipula que el delito solo se materializa si la propuesta de encuentro "*ha sido seguida de actos materiales que conduzcan a dicha reunión*" sin bastar solo el contacto, sino que deben haberse producido actos orientados a que se concrete un encuentro.(24)

Es que el derecho penal liberal tiene como presupuesto para punir una conducta que la misma lesione algún bien jurídico de un tercero; esto queda claro si analizamos los principios de reserva y de lesividad, enunciados de manera expresa en nuestra Constitución Nacional, en virtud de los cuales las acciones de un ciudadano que no lesionen intereses de terceros y que no ofendan al orden y la moral pública están exentas de las autoridades de los magistrados(25). Entonces, de ello se desprende que el ciudadano es responsable por su conducta en la medida que ella afecta a la sociedad: si su conducta no produce un daño o una lesión a terceros no corresponde que sea castigada.

Dicho esto, corresponde hacer un análisis de las diferentes etapas que se desarrollan desde que se concibe la idea de cometer un acto ilícito hasta la consumación del mismo.

(22) Tazza, Alejandro O.: "El delito de *grooming*" - LL - 7/3/2014

(23) Grisetti, Ricardo A.: "El *grooming*. Una nueva modalidad delictual" - LL - 1/7/2016 - pág. 1

(24) Vaninetti, Hugo A.: "Inclusión del '*grooming*' en el Código Penal" - LL - 16/12/2013 - pág. 1 - LL2013-F, 1200 - LLP 2014 (marzo)

(25) **Art. 19** - *Las acciones privadas de los hombres que de ningún modo ofendan al orden y a la moral pública, ni perjudiquen a un tercero, están sólo reservadas a Dios, y exentas de la autoridad de los magistrados. Ningún habitante de la Nación será obligado a hacer lo que no manda la ley, ni privado de lo que ella no prohíbe*

Estas etapas están caracterizadas por el comportamiento del autor orientado a la comisión de un delito, sin que esto implique que estos actos sean delito por sí mismos. El hecho de que puedan o no considerarse de tal manera dependerá de si lesionan o no algún bien jurídico por sí mismos y si se encuentran o no tipificados dentro de nuestro derecho.

Entre estas etapas deben distinguirse las que no trascienden el pensamiento, que por regla no son punibles, y aquellas que suponen la materialización de acciones externas, que pueden ser punibles o no.(26)

En relación con las etapas internas que no trascienden de la esfera psicológica del individuo, la primera fase es la ideación, que puede subdividirse en cuatro sub-etapas: el nacimiento de la idea, un examen de factibilidad, un examen de pros y contras de la conducta ideada y la decisión, que podrá dar lugar a un desistimiento o a que se siga adelante con el plan(27). Esta etapa no será punible debido a que el pensamiento por sí mismo no es punible, dado que no puede causar una lesión a un bien jurídico.

Dentro de los actos que trascienden el plano de los pensamientos se presentan tres tipos de actos: los preparatorios, los de ejecución y los de consumación. Un acto se considera preparatorio cuando, de manera preliminar a la concreción del delito, el individuo comienza a procurarse los medios necesarios para realizar la acción disvaliosa.

Se dice que un acto es de ejecución cuando pone de manifiesto la voluntad de llevar a cabo el delito que ha ideado.

Finalmente tenemos los actos de consumación, que son aquellos que permiten la realización del tipo objetivo, es decir, son todos los actos que están descriptos en el tipo expresado en la parte especial del CP.(28)

Ahora bien, en relación con los actos preparatorios, la regla general es que no son punibles, salvo cuando estos actos estén contenidos en otro tipo penal, en cuyo caso el sujeto no va a ser penado por haber preparado un hecho ilícito, sino porque consumó otro delito previamente.

El fundamento de que no generen responsabilidad penal los actos preparatorios es que de ellos no puede inferirse, más allá de toda duda razonable, que este acto en cuestión forme parte de un plan delictivo. Si tomamos como referencia el delito que motiva este trabajo, vemos que no todo el que inicia un contacto con un menor de edad busca cometer un delito en contra de su integridad sexual. En relación con estos actos, Zaffaroni distingue claramente entre los actos ejecutivos, que serán punibles por ser actos de tentativa propiamente dichos -y por lo tanto susceptibles de reproche penal- de los preparatorios, que regularmente serán impunes.(29)

Sin embargo, el citado autor reconoce que no existen, dentro del marco de las teorías que buscan delimitar entre actos preparatorios y ejecutivos, soluciones satisfactorias al problema planteado y sostiene que se trataría de un problema que debe ser resuelto por la parte especial, debiendo el propio legislador establecer qué actos serán punibles.

(26) Righi, Esteban: "Derecho penal - Parte general" - 2ª reimpresión - Bs. As. - Ed. Abeledo Perrot - 2010 - pág. 408

(27) Righi, Esteban: "Derecho penal - Parte general" - 2ª reimpresión - Bs. As. - Ed. Abeledo Perrot - 2010 - pág. 408

(28) Righi, Esteban: "Derecho penal - Parte general" - 2ª reimpresión - Bs. As. - Ed. Abeledo Perrot - 2010 - pág. 409

(29) Zaffaroni, Eugenio R.: "Manual de derecho penal - Parte general" - 9ª reimpresión - Bs. As. - 1999 - Ed. Ediar - pág. 606

Continuando, debemos resaltar la delimitación y definición del tipo penal que resulta poco feliz, sobre todo teniendo en cuenta que previo a su sanción el proyecto fue discutido en la Cámara de Diputados, donde se modificó el texto de la siguiente manera: "*Será penada con prisión de tres meses a dos años la persona mayor de edad, que por medio de comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos, le requiera de cualquier modo a una persona menor de trece años, que realice actividades sexuales explícitas o actos con connotación sexual o le solicite imágenes de sí misma con contenido sexual. La misma pena se aplicará a la persona mayor de edad que realizare las acciones previstas en el párrafo anterior con una persona mayor de trece y menor de dieciséis años, cuando mediare engaño, abuso de autoridad o intimidación*".

Como se ve, el texto modificado por Diputados resultaba mucho más preciso y adecuado que el que se encuentra actualmente en vigencia.

También vemos que en esta definición se delimita la edad de la víctima de manera precisa. Recordemos que para el ordenamiento argentino una persona mayor de dieciséis años ya puede consentir una relación sexual con un mayor, con lo cual resulta propio del caso que se entienda como víctimas de este delito solo a los menores de trece años y a aquellos que se encuentran entre el rango comprendido entre trece y dieciséis.

Aquí debemos mencionar el tratamiento que se le dio en el anteproyecto del CP del año 2013, donde se lo establecía en el inciso segundo del artículo 133 de la siguiente manera: "*Será penado con prisión de uno (1) a cinco (5) años, el mayor de edad que tomare contacto con un menor de trece años, mediante conversaciones o relatos de contenido sexual, con el fin de preparar un delito de este Título*".(30)

Como se ve, en esta redacción se distingue claramente la calidad de mayor del autor de la figura típica; establece además que el sujeto pasivo debe ser un menor de trece años, tomando esto de la redacción del artículo 183 del Código Penal español; mantiene la descripción de la figura típica en relación con la conducta exigida y toma contacto con la finalidad de cometer un delito contra la integridad y la libertad sexual, sin distinguir el medio de comunicación elegido.

La comisión, en la exposición de motivos de este anteproyecto, explica que se está ante un acto preparatorio, que si alcanza el nivel de comienzo de ejecución de otro delito desaparece en función de las reglas del concurso aparente.(31)

b) Aspectos relevantes de la previsión normativa del *grooming* en la Argentina

De lo expuesto, vemos que en todos los casos la figura típica en nuestro derecho positivo consiste en un delito de peligro, caracterizado por el medio por el cual es cometido, que exige un componente subjetivo dado por la intención de concretar el encuentro, quedando fuera del tipo las meras conversaciones de contenido sexual.

Entonces, podemos decir que estamos ante un delito de doble acción, ya que requiere que el autor contacte a un menor en primer lugar y que luego busque concretar un encuentro, con la finalidad de cometer un delito contra la integridad sexual.

(30) "Anteproyecto de Código Penal de la República Argentina". Redactado por la Comisión para la Elaboración del Proyecto de Ley de Reforma, Actualización e Integración del Código Penal de la Nación [Dto. (PEN) 678/2012]

(31) Castro, Julio: "Delitos contra la integridad y libertad sexual" - Ed. Rubinzal-Culzoni - conf. Revista de Derecho Penal - Bs. As. - 2014 - N° extraordinario - pág. 375

Es dable afirmar que nos encontramos ante la tipificación como delito de meros actos preparatorios, con la consabida dificultad probatoria que implica su equivocidad, así como el peligro que significa la constante ampliación del universo punitivo, que parece no tener coto.

El tipo penal no especifica cuál delito debe estar motivado para cometer el autor, basta que afecte la integridad sexual de la víctima, pudiendo tratarse de cualquiera de los que se encuentran legislados en nuestro CP vigente.

Como se ve, la complicación al momento de comprobar que se está ante este delito va a estar siempre en lograr probar el elemento subjetivo del tipo penal, lo que lleva a que se vaya a imponer una pena basándose en meras suposiciones a partir del análisis de los contenidos de las charlas.

El dolo exigido por el tipo es el dolo directo: no puede ser de otra manera debido a la presencia de este elemento subjetivo. En consecuencia, no se admite ni el dolo eventual ni la forma culposa.[32]

V - EL *GROOMING* EN EL DERECHO COMPARADO

a) El *grooming* de acuerdo con los tratados internacionales

Lo primero que debemos analizar al hablar del *grooming* en el contexto internacional son las fuentes convencionales. La principal fuente de definiciones que corresponde mencionar es el Convenio sobre Cibercriminalidad de Budapest, celebrado en noviembre del 2001 y al que la República Argentina ha adherido en el año 2010.

Dicho convenio surge de la voluntad y la convicción de los Estados parte de que, conforme se declara en su preámbulo, "*… la lucha contra la ciberdelincuencia requiere una cooperación internacional reforzada, rápida y eficaz en materia penal*".

En el citado convenio, no se define expresamente el *grooming*, dado que no presenta una estructura de tipos penales bien definidos, sino más bien expresa descripciones genéricas de conductas no deseables y lesivas respecto de determinados bienes jurídicos, a los fines de que los signatarios sean quienes determinen, de acuerdo a las reglas de su derecho positivo, las respuestas del sistema penal a dichas conductas.

Sí vale mencionar respecto de dicho convenio que entiende como menores a toda persona que no haya cumplido 18 años de edad, aunque hace la salvedad de que los Estados firmantes podrán estipular límites de edad inferior, aunque este no podrá ser inferior a 16 años.

En nuestro derecho, considero que, en relación con el *grooming,* es este límite de 16 años el que debe ser tomado en cuenta, debido a que si se considera que una persona de esa edad se encuentra en condiciones de ofrecer su consentimiento para mantener relaciones sexuales, bien puede entenderse que es capaz de decidir si desea o no entablar una relación con una persona mayor. Sin embargo, el tipo penal no lo dice expresamente.

En los casos en los cuales la relación sea evidentemente no consentida o que se intente lograr mediante amenazas o violencia psicológica, entiendo que se estará ante la comisión de otros tipos penales, por ejemplo extorsión, abuso sexual, etc.

(32) Grisetti, Ricardo A.: "El *grooming*. Una nueva modalidad delictual" - LL - 1/7/2016 - pág. 1

Respecto a la definición del *grooming* como delito, debemos mencionar que el primer convenio en incluirlo fue el Convenio del Consejo de Europa para la Protección de los Niños frente a la Explotación y Abuso sexual, del 25/10/2007, también conocido como Convenio de Lanzarote. Este convenio, en su artículo 23, expresa que cada uno de los Estados parte deberá contribuir a tipificar como delito la conducta de un adulto que, mediante el empleo de tecnologías de la información y la comunicación, proponga un encuentro a niños que no hayan alcanzado la edad fijada como mínima por ese estado para que una relación sexual se encuentre permitida. Además exige que en dicho encuentro el adulto tenga la intención de cometer algún delito en contra de la integridad sexual de la víctima, pero establece también como requisito que la propuesta haya sido seguida de acciones materiales tendientes a concretar el encuentro.

Como se observa al comparar con el texto vigente en nuestro derecho, se agrega a la intención de cometer un delito contra la integridad sexual, o elemento subjetivo, otro elemento de carácter objetivo, como lo son los actos orientados a la concreción del encuentro.

b) El *grooming* en el Código Penal español

A partir del Convenio de Lanzarote se introdujo en España el delito de *grooming*, para lo cual se reformó el código penal de dicho país incluyendo el tipo en el artículo 183 bis del citado cuerpo normativo.

El artículo en cuestión establece que el autor de este delito puede ser cualquier persona que contacte y proponga concertar un encuentro (propuesta que debe ir acompañada de actos materiales orientados al acercamiento), utilizando como medio internet, teléfono o cualquier otra de las tecnologías de la información y la comunicación (TIC), con el fin de cometer delitos que lesionen la indemnidad sexual de la víctima.

Este tipo penal se agrava cuando el autor se vale para obtener el acercamiento de coacción, intimidación o engaño.

Como vemos, al igual que en nuestro derecho vigente, respecto del autor el tipo no distingue entre adultos y menores, pero sí agrega el requisito objetivo de los actos materiales encaminados a concretar el encuentro.

De lo dicho surge que para el derecho español, como para el nuestro, el delito puede ser cometido tanto por adultos como por menores, por lo que se está ante una verdadera extensión del ámbito de punición respecto de la norma internacional.[33]

En cuanto a la conducta típica, coincide el texto español con los tratados precedentes en exigir como requisitos la propuesta de encuentro acompañada por actos materiales orientados a la producción del mismo[34]. En cambio, en el derecho argentino se ha tipificado, como ya hemos mencionado, que exista una propuesta de encuentro sin la exigencia de los actos materiales que lleven a su concreción, aunque materialmente podría decirse que este tipo de actos son los indicios del requisito subjetivo que tiene el tipo penal.

(33) Cugat Mauri, Miriam: "La tutela penal de los menores ante el online grooming: entre la necesidad y el exceso" en Riquert, Marcelo A. (Coord.): "Ciberdelitos. *Grooming. Stalking. Bullyng. Sexting.* Ciberodio. Propiedad intelectual. Problemas de perseguibilidad. Ciberpornografía infantil" - Ed. Hammurabi - Bs. As. - 2014 - pág. 253

(34) Cugat Mauri, Miriam: "La tutela penal de los menores ante el *online grooming*: entre la necesidad y el exceso" en Riquert, Marcelo A. (Coord.): "Ciberdelitos. *Grooming. Stalking. Bullyng. Sexting.* Ciberodio. Propiedad intelectual. Problemas de perseguibilidad. Ciberpornografía infantil" - Ed. Hammurabi - Bs. As. - 2014 - pág. 253

En lo que encontramos coincidencia en todas las descripciones típicas es respecto de los medios utilizados para el contacto: todos los cuerpos normativos citados especifican que deben utilizarse medios relacionados con las tecnologías de la información y comunicación.

Debemos adherir a la acertada crítica realizada al tipo penal español en relación con que dispuso que la coacción, el engaño y la intimidación formen parte del tipo agravado, produciendo un vaciamiento de contenido respecto del tipo básico(35). Como ya hemos expresado, la utilización de engaños, intimidación y diversas formas de coacción son elementos básicos de este delito, de conformidad con las definiciones internacionales. En consecuencia, para la legislación española prácticamente en todos los casos se va a estar frente a la figura agravada.

En relación con el requisito subjetivo, todas las legislaciones y fuentes convencionales exigen la intención del autor de cometer un delito de índole sexual con un menor que no haya alcanzado la madurez sexual. La diferencia se encuentra en que en los tratados internacionales se hace referencia expresa a la producción de pornografía infantil y al requisito de que los actos sean realizados contra menores que no han alcanzado la referida madurez sexual.(36)

La crítica que se hace de parte de la mayoría de la doctrina a la formulación del tipo en la ley española es que existe un vacío en relación con los menores mayores de trece años, que son los que tienen mayor acceso a internet(37). Esta limitación surge del hecho de que se considera, de acuerdo a la legislación española, que un menor de edad ha alcanzado la madurez sexual a los trece años, aunque debe destacarse que existen proyectos para elevar el límite de edad, actualmente en discusión en el parlamento español.

Otra coincidencia que se presenta en todos los instrumentos revisados hasta ahora es que el contacto sin voluntad de que se produzca el encuentro resulta atípico.

c) Recepción en el derecho latinoamericano

Resulta destacable que el Convenio sobre Cibercriminalidad de Budapest, si bien emana de un organismo europeo, el Consejo de Europa, ha influido en legislaciones de otros países. En particular, ha sido receptado por el derecho vigente de los países miembros del MERCOSUR.

Esto resulta posible en gran medida debido a que no especifica tipos penales que deben ser receptados, sino más bien utiliza formulas genéricas y abiertas, con sugerencias

(35) Cugat Mauri, Miriam: "La tutela penal de los menores ante el *online grooming*: entre la necesidad y el exceso" en Riquert, Marcelo A. (Coord.): "Ciberdelitos. *Grooming. Stalking. Bullyng. Sexting.* Ciberodio. Propiedad intelectual. Problemas de perseguibilidad. Ciberpornografía infantil" - Ed. Hammurabi - Bs. As. - 2014 - pág. 267

(36) Cugat Mauri, Miriam: "La tutela penal de los menores ante el *online grooming*: entre la necesidad y el exceso" en Riquert, Marcelo A. (Coord.): "Ciberdelitos. *Grooming. Stalking. Bullyng. Sexting.* Ciberodio. Propiedad intelectual. Problemas de perseguibilidad. Ciberpornografía infantil" - Ed. Hammurabi - Bs. As. - 2014 - pág. 268

(37) Cugat Mauri, Miriam: "La tutela penal de los menores ante el *online grooming*: entre la necesidad y el exceso" en Riquert, Marcelo A. (Coord.): "Ciberdelitos. *Grooming. Stalking. Bullyng. Sexting.* Ciberodio. Propiedad intelectual. Problemas de perseguibilidad. Ciberpornografía infantil" - Ed. Hammurabi - Bs. As. - 2014 - pág. 270

en relación con alternativas para que cada uno de los signatarios adapte estas sugerencias a su estructura de derecho local.(38)

1. Chile

Un ejemplo relacionado con el delito aquí tratado nos lo da el Código Penal chileno, que incluyó este delito en su artículo 366 quáter mediante la ley de *grooming* del 2011(39), el cual en principio penaba la comisión de conductas de contenido sexual ante menores.

A partir de la sanción de la citada ley, incluye dentro del marco punible a aquel que comete conductas sexuales ante menores a distancia, utilizando medios electrónicos.

El legislador chileno, de la misma manera que el español, ha considerado que corresponde que el engaño respecto de la edad o identidad del autor estén incluidos en la figura agravada, pero no incorpora a este la coacción ni las amenazas, dejándolas dentro de la figura básica.

2. Brasil

El escenario en Brasil es similar al descripto en Chile. El delito de *grooming* se incluyó en el Estatuto del menor y Adolescente (ECA, L. 8069/1990) a partir de la ley 11829/2008, que lo tipifica en el artículo 241-D.

La redacción del tipo penal es bastante similar a la de nuestro país. La conducta descripta es el contacto con un menor a través de cualquier medio de comunicación con la finalidad de realizar un acto de contenido sexual.(40)

Como vemos, se asemeja a lo dispuesto en el artículo 131 de nuestro CP, respecto de que el contacto puede darse utilizando cualquier medio de comunicación, no limitando al contacto con medios informáticos.

Al igual que en nuestra legislación, tampoco especifica que el autor debe ser una persona mayor de edad, por lo que entendemos que un menor de edad que realice la acción típica podrá ser considerado como autor del delito.

(38) Riquert, Marcelo A: "Repensando cómo funciona la ley penal en el ciberespacio" en Riquert, Marcelo A. (Coord.): "Ciberdelitos. *Grooming. Stalking. Bullyng. Sexting*. Ciberodio. Propiedad intelectual. Problemas de perseguibilidad. Ciberpornografía infantil" - Ed. Hammurabi - Bs. As. - 2014 - pág. 17

(39) **Art. 366 quáter** - "*El que, sin realizar una acción sexual en los términos anteriores, para procurar su excitación sexual o la excitación sexual de otro, realizare acciones de significación sexual ante una persona menor de catorce años, la hiciere ver o escuchar material pornográfico o presenciar espectáculos del mismo carácter, será castigado con presidio menor en su grado medio a máximo. Si, para el mismo fin de procurar su excitación sexual o la excitación sexual de otro, determinare a una persona menor de catorce años a realizar acciones de significación sexual delante suyo o de otro o a enviar, entregar o exhibir imágenes o grabaciones de su persona o de otro menor de 14 años de edad, con significación sexual, la pena será presidio menor en su grado máximo. Quien realice alguna de las conductas descritas en los incisos anteriores con una persona menor de edad pero mayor de catorce años, concurriendo cualquiera de las circunstancias del numerando 1º del artículo 361 o de las enumeradas en el artículo 363 o mediante amenazas en los términos de los artículos 296 y 297, tendrá las mismas penas señaladas en los incisos anteriores. Las penas señaladas en el presente artículo se aplicarán también cuando los delitos descritos en él sean cometidos a distancia, mediante cualquier medio electrónico. Si en la comisión de cualquiera de los delitos descritos en este artículo, el autor falseare su identidad o edad, se aumentará la pena aplicable en un grado*"

(40) **Art. 241-D** - *Aliciar, assediar, instigar ouconstranger, por qualquermeio de comunicação, criança, com o fim de comelapraticar ato libidinoso*: (Incluído pela Lei nº 11.829, de 2008)

Lo que debe destacarse es que Brasil fue el primer país de la región en incluir el delito. Lo incorporó en el año 2008; Chile, en el año 2011 y nuestro país, en el año 2013.

3. Perú

En Perú se tipificó con la sanción de la ley de delitos informáticos, que lo incorporó en su artículo 5[41]. En la legislación peruana se pena establecer el contacto con un menor de edad con la finalidad de obtener material pornográfico o con el propósito de llevar a cabo actividades sexuales que lesionen la indemnidad o libertad sexual del menor.

El artículo prevé dos supuestos: en primer lugar, el contacto con un menor de catorce años y, en segundo, el contacto con menores que tienen entre catorce y dieciocho años.

En Perú tampoco se ha dispuesto que el delito deba ser cometido por un adulto, pero se ha establecido que el contacto sea realizado por internet o un medio análogo, con lo que ha quedado un poco restringido el catálogo de medios de comunicación que pueden usarse para cometer el delito.

La coincidencia que encontramos en todas las legislaciones mencionadas es que, al igual que en nuestro código penal y en el de España, se ha adelantado la punibilidad a actos preparatorios, por lo que las mismas observaciones que realizamos al respecto al momento de analizar la redacción en nuestro derecho pueden aplicarse.

Se ve que en todas las legislaciones mencionadas es notoria la influencia que han tenido tanto el Convenio de Budapest como el Convenio de Lanzarote, con lo cual podemos hablar de una gestación de una suerte de política criminal internacional, donde ha primado la visión europea respecto de la respuesta estatal a este fenómeno.

VI - CONCLUSIONES

En el presente trabajo se han enunciado las dificultades que conlleva la previsión legal del *grooming,* así como también las de índole probatoria, que surgen de la naturaleza del medio en que se comete este tipo penal o de las propias limitaciones que poseen los Estados para su investigación.

Se ha comparado la manera en que ha sido receptado y creado este delito en la República Argentina con otros países de idéntica raigambre jurídica como España, Chile, Brasil y Perú.

En relación con España, hemos visto que, al igual que en Argentina, la previsión legal respecto del autor no distingue entre adultos y menores, lo que significa un apartamiento y ampliación punitiva en relación con la normativa internacional, aunque en ese país sí se ha agregado el requisito objetivo de la existencia de actos materiales encaminados a concretar el encuentro. Además, España ha vaciado la figura básica, incurriendo siempre en la agravada al no requerir engaño, intimidación o coacción. En esto último solamente se distingue la tipificación chilena.

(41) **Art. 5** - "*El que a través de internet u otro medio análogo contacta con un menor de catorce años para solicitar u obtener de él material pornográfico, o para llevar a cabo actividades sexuales con él, será reprimido con pena privativa de libertad no menor de cuatro ni mayor de ocho años e inhabilitación conforme a los numerales 1, 2 y 4 del artículo 36 del Código Penal.*

Cuando la víctima tiene entre catorce y menos de dieciocho años de edad y medie engaño, la pena será no menor de tres ni mayor de seis años e inhabilitación conforme a los numerales 1, 2 y 4 del artículo 36 del Código Penal"

Brasil no ha limitado el medio comisivo a los informáticos, lo que implica la desnaturalización de la figura, que necesariamente y desde lo conceptual requiere su comisión por esos medios. Asimismo, tiene el mismo problema que Argentina y España sobre la posibilidad de que el autor sea tanto un menor como un mayor.

Todas las regulaciones tratadas sufren como objeción más sólida, desde el punto de vista del derecho penal, la punición de un acto de naturaleza preparatorio, y por lo tanto equívoco, del contacto con el menor, lo que podría afectar entonces el principio de legalidad al abarcar posibles imputaciones por acciones que no son necesariamente dirigidas solo a un fin sexual.

Sin embargo, este no ha sido el único problema detectado en la redacción del tipo. Entre otros, se ha indicado la dudosa legitimidad de la que pudiere gozar la redacción de un tipo de peligro que prescinde de la efectiva lesión de un bien jurídico mediante la conducta incriminada, la indefinición del concepto de menor o la posibilidad de que el sujeto activo pueda ser tanto un menor como un mayor, lo que a todas luces no ha sido lo que ha buscado captar el legislador.

Quizás los escollos de tipo probatorio, a los que se suman los de índole legal, sean el motivo de la muy escasa jurisprudencia que puede relevarse en la actualidad. Lo real es que la cantidad de denuncias, por más percepción que tenga la sociedad de su cantidad, por el contrario, es muy escasa.

Finalmente, y por otro andarivel, de acuerdo con los argumentos vertidos, también es válido afirmar que por más que el fin que la generó sea loable, la previsión normativa del *grooming,* al menos en la República Argentina, es inconstitucional, pues viola los principios de legalidad, de reserva y de lesividad.

Delitos sexuales en la era digital

Mara Resio(*)

"La palabra 'digital' refiere al dedo (digitas), que ante todo cuenta. *La cultura digital descansa en los dedos que cuentan".*(1)

I - INTRODUCCIÓN

El nuevo mundo de la tecnología abre un inmenso abanico de posibilidades. Riesgos y beneficios se entrecruzan en la web. La comunicación se transformó con la aparición de internet y las redes sociales y, por lo tanto, la manera de relacionarse de los individuos mutó. *"Cojeamos tras el medio digital, que por debajo de la decisión consciente, cambia decisivamente nuestra conducta, nuestra percepción, nuestra sensación, nuestro pensamiento, nuestra convivencia".*(2)

Las normas de convivencia de las sociedades y los paradigmas culturales también sufrieron el cambio. La necesidad de actualización es inminente para poder dar soluciones a los novedosos problemas. Cuando los delitos son cometidos a través de formatos digitales, la justicia se encuentra con lagunas, y el derecho penal tradicional no basta para dar respuestas.

(*) Abogada (UBA). Periodista (TEA). Especialización en Derecho, trabajo de investigación: "La delincuencia juvenil relatada por los medios de comunicación en Argentina y España" (Universidad de Salamanca). Adjunta en el Seminario de Genocidio (IUNMA). Ayudante de segunda de la materia Elementos de Derecho Penal y Procesal Penal, cátedra Virgolini - Silvestroni (UBA)

(1) Byung-Chul Han: "En el enjambre" - Herder Editorial - Barcelona - 2014 - pág. 1

(2) Byung-Chul Han: "En el enjambre" - Herder Editorial - Barcelona - 2014 - pág. 6

La legislación argentina está en pleno proceso de renovación. Actualmente las leyes prevén que los delitos pueden perpetrarse a través del uso de medios informáticos o dispositivos electrónicos.

De a poco, aparecieron figuras penales relacionadas con la temática. La ley 26388 es conocida como la ley de delitos informáticos y siguió los lineamientos dispuestos en el Convenio sobre la Ciberdelincuencia de Budapest, que facilita la colaboración internacional para perseguir delitos trasnacionales. En la Argentina, la ley 27411 adhiere al Convenio mencionado, el cual es un marco para legislar los delitos electrónicos y la evidencia digital.

Años después, se sancionó la ley 26904 que incorpora al Código Penal (art. 131) el delito de ciberacoso sexual o *"grooming"*, *"que abarca conductas tendientes a contactar por medio de comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos, a una persona menor de edad con el propósito de cometer cualquier delito contra su integridad sexual"*.[3]

La reciente sanción de la ley 27436[4] modificó el artículo 128 del Código Penal, al tipificar la tenencia de pornografía infantil.

Pese a que se comenzó a legislar sobre las consecuencias del uso de las nuevas tecnologías de la comunicación y la información, todavía falta mucho camino por recorrer. La necesaria adecuación de las normas a los tiempos actuales permitiría resguardar adecuadamente los derechos fundamentales reconocidos en la Constitución Nacional.

El país continúa en la búsqueda de adaptarse a la realidad tecnológica. A propósito de esto, se dictó el decreto 103/2017 para crear una Comisión presidida por el juez Mariano Borinsky y conformada por jueces y fiscales del Poder Judicial de la Nación y de las provincias, miembros del Ministerio de Justicia y del Ministerio de Seguridad y Desarrollo Social, profesores universitarios y abogados especialistas en el derecho penal. La Comisión ideó el Anteproyecto para la Reforma del Código Penal, el cual establece en el Título XXVI: "Delitos informáticos", el Capítulo I: "Atentados a través de medios informáticos". Allí introduce el artículo 493, novedoso para la Argentina, pero que ya está previsto en otras partes del mundo. La norma dispone lo siguiente: *"Se impondrá prisión de seis (6) meses a dos (2) años o seis (6) a veinticuatro (24) días-multa, al que sin autorización de la persona afectada difundiere, revelare, enviare, distribuyere o de cualquier otro modo pusiere a disposición de terceros imágenes o grabaciones de audio o audiovisuales de naturaleza sexual, producidas en un ámbito de intimidad, que el autor hubiera recibido u obtenido con el consentimiento de la persona afectada, si la divulgación menoscabare gravemente su privacidad.*

La pena será de prisión de uno (1) a tres (3) años:

1. *Si el hecho se cometiere por persona que esté o haya estado unida a la víctima por matrimonio, unión convivencial o similar relación de afectividad, aun sin convivencia.*
2. *Si la persona afectada fuere una persona menor de edad.*
3. *Si el hecho se cometiere con fin de lucro".*

Mientras el Capítulo II regula el daño informático, el Capítulo III trata sobre hurto y fraude informáticos, el IV es sobre el acceso ilegítimo y el V prevé que si un funcionario público intervino en alguno de los delitos informáticos mencionados se le impondrá, además, pena de inhabilitación especial por el doble del tiempo de la condena a prisión.

(3) BO: 11/12/2013

(4) BO: 23/4/2018

Asimismo, existen proyectos legislativos[5] con el propósito de penar *"la publicación y/o difusión de imágenes no consentidas de desnudez total o parcial y/o videos de contenido sexual o erótico de personas"*. Uno de ellos, el Proyecto S-2119/2016, tiene media sanción de la Cámara de Senadores y fue modificado en la Cámara de Diputados.

La norma original del Proyecto prevé la incorporación del artículo 155 bis al Código Penal: *"Será reprimido con la pena de prisión de seis (6) meses a cuatro (4) años, el que hallándose en posesión de imágenes de desnudez total o parcial y/o videos de contenido sexual o erótico de una o más personas, las hiciere pública o difundiere por medio de comunicaciones electrónicas, telecomunicaciones, o cualquier otro medio o tecnología de transmisión de datos, sin el expreso consentimiento de la o de las mismas para tal fin, aun habiendo existido acuerdo entre las partes involucradas para la obtención o suministro de esas imágenes o video. La persona condenada será obligada a arbitrar los mecanismos necesarios para retirar de circulación, bloquear, eliminar o suprimir, el material de que se tratare, a su costa y en un plazo a determinar por el juez"*.

Por su parte, Diputados dispuso la modificación del artículo 155 del Código Penal actual y agregó: *"...la pena será de pesos cincuenta mil ($ 50.000) a pesos trescientos mil ($ 300.000) para el que, por cualquier medio, y sin autorización, difundiere, divulgare, publicare, distribuyere o de cualquier manera pusiere al alcance de terceros un video, imagen o cualquier material sobre desnudos o semidesnudos de otra persona, o material de contenido erótico o sexual, que sea privado, cuando menoscabe la intimidad de la víctima. Para quien haya realizado la conducta descrita en el párrafo anterior trasgrediendo por primera vez la presunta expectativa de intimidad, la pena será de tres (3) meses a tres (3) años de prisión. Está exento de responsabilidad penal el que hubiere obrado con el propósito inequívoco de proteger un interés público"*.

Actualmente en la Argentina la difusión sin autorización de imágenes íntimas no está penalizada, excepto si se accede indebidamente a correos electrónicos, computadoras o se utiliza el *malware* para captar claves y de ese modo se adquiere el contenido privado.

Al año siguiente de esa propuesta se presentó otro Proyecto -3862-D-2017-, también para penalizar la difusión no consentida de material íntimo a través de las plataformas digitales y, además, sancionar el acoso virtual. Entre los fundamentos se destaca lo siguiente: *"El vacío legislativo respecto de los derechos de los particulares a la intimidad y la privacidad requiere del desarrollo de una nueva etapa en el avance legislativo sobre las nuevas realidades que nos tocan afrontar mediante el uso de las nuevas tecnologías"*. La norma plantea la incorporación de los artículos 131 bis, ter y quater al Código Penal, y la modificación del artículo 153 bis del Código Penal.

En el mismo orden de ideas, los representantes del Consejo de Procuradores Fiscales, Defensores y Asesores Generales de la República Argentina presentaron al Ministerio de Justicia y Derechos Humanos de la Nación un documento con reformas al Código Penal. En el escrito proponen añadir nuevas definiciones delictuales, como: el acoso -*stalking*-, el maltrato reiterado, la agresión psicológica y el *sexting*[6]. Además, plantean la creación de nuevas figuras que sancionen el incumplimiento de órdenes judiciales de restricción de acercamiento, el agravamiento de las condenas de delitos preexistentes cuando las víctimas sean mujeres y una mejora a la protección de la integridad sexual. Pese a las nuevas necesidades de proteger los derechos, cabe recordar que el derecho penal es la

(5) S-2180/15, 5893-D-2016, entre otros

(6) Musse, Valeria: "Piden crear nuevas figuras penales contra las agresiones a las mujeres" - La Nación - 20/12/2016

ultima ratio del poder punitivo del Estado. Sin embargo, las leyes actuales no satisfacen las problemáticas que introduce el uso de la tecnología. La doctora Nora Cherñavsky, profesora adjunta de la Universidad de Buenos Aires y especialista en investigación del derecho informático y ciberdelito, sostiene: *"el medio digital, por sus características técnicas y el anonimato que confiere a sus usuarios, también brinda un espacio de oportunidad favorable al incremento de conductas inapropiadas, disvaliosas e incluso delictivas"*. Hace referencia a *"los ciberacosos, hostigamientos, amenazas y extorsiones, que encuentran en este entorno digital el ambiente propicio para llegar en menor tiempo a un número mayor e indeterminado de víctimas"*[7]. Conductas de contenido sexual merecedoras de reproche penal, como el *sexting*, el *stalking*, la pornovenganza y la *sextorsión*, se propagan en formatos digitales, y todavía hoy en la Argentina no encuentran un reparo justo.

II - *SEXTING*

Uno de los peligros que surgieron, dentro de las tecnologías de la información y la comunicación (TIC), son las prácticas de *sexting*. La palabra representa la contracción gramatical de *sex* -sexo- y *texting* -envío de mensajes de texto-. El término hace referencia al envío de contenidos eróticos o pornográficos por medio de teléfonos móviles. En un principio solo se lo vinculaba con el envío de SMS de naturaleza sexual, *"pero con la extensión de las capacidades multimedia de los dispositivos móviles, han aumentado los envíos de fotografías y vídeos, a los cuales se les sigue aplicando el mismo término"*.[8]

El Observatorio de la Seguridad de la Información estableció qué implica esta práctica: *"la difusión o publicación de contenidos (principalmente fotografías o vídeos) de tipo sexual, producidos por el propio remitente, utilizando para ello el teléfono móvil u otro dispositivo tecnológico. El contenido de carácter sexual, generado de manera voluntaria por su autor, pasa a manos de otra u otras personas, pudiendo entrar en un proceso de reenvío masivo multiplicándose su difusión"*[9]. Por su parte, Florencia Galeazzo identifica a las redes sociales como el medio por el cual se hace el intercambio de fotografías de índole sexual.[10]

Las primeras veces que se habló sobre esta conducta entre jóvenes de los Estados Unidos fue en la revista Sunday Telegraph, en 2005.[11]

En la Argentina, diversas legislaciones provinciales establecen mecanismos contra el sexting entre menores de edad. La ley 5385[12] de Catamarca aborda, desde el ámbito escolar, el uso seguro de internet y de las nuevas TIC. El Programa de Capacitación Escolar y Familiar tiene como objeto que se cree *"un programa de capacitación en el ámbito*

(7) Centro de Ciberseguridad de CABA: "Las mujeres y la ciberseguridad" - Boletín N° 35 - 8/3/2018

(8) Ghersi, Carlos A.: "Daño al derecho personalísimo de privacidad en internet" - Microjuris - 18/3/2014

(9) Mendoza Calderón, Silvia: "El derecho penal frente a las formas de acoso a menores. *Bullying, ciberbullying, grooming y sexting*" - Ed. Tirant lo Blanch - España - 2013 - pág. 169

(10) Galeazzo, Florencia: "Efectos del acoso escolar, cyberbullying y grooming en la responsabilidad parental" - ERREIUS - Temas de Derecho de Familia, Sucesiones y Bioética - octubre/2017 - Cita digital IUSDC285472A

(11) Cornaglia, Carlos A. (Dir.): "Abuso sexual de menores. Criminal plaga" - 1ª ed. - Ed. Alveroni - Córdoba - 2011 - pág. 232

(12) BO: 27/1/2015

escolar y familiar para que niñas, niños y adolescentes puedan incorporar herramientas idóneas que les permitan un uso seguro del internet y de las nuevas tecnologías de la información y la comunicación (NTIC)".

En el artículo 2 de la ley se establecen los destinarios, que son niñas, niños y adolescentes del territorio de la Provincia, en edad de escolarización; docentes, profesores y personal del sistema educativo provincial de establecimientos públicos y privados; y la familia de los menores.

El siguiente artículo detalla la terminología de *sexting* como el *"intercambio de material de contenido sexual, sea en imágenes o videos, a través de correo electrónico o telefonía celular".*

Por su parte, La Rioja sancionó la ley 9692[13], la cual creó el Programa Provincial de Concientización, Prevención y Difusión de Información contra el *"grooming, sexting y ciberbullying".* Estableció que el Ministerio de Educación, Ciencia y Tecnología de la Provincia sea la autoridad de aplicación. Define a la conducta de sexting como *"el envío de contenidos eróticos o pornográficos a través de teléfonos móviles"* (art. 4).

El programa estipula que los establecimientos educativos públicos y privados deben promover el tratamiento de las temáticas en el desarrollo de las políticas públicas provinciales. Además, prevé que se realicen actividades y capacitaciones de concientización para que los menores conozcan los riesgos propios de internet y adquieran herramientas para evitarlos. También estipula el asesoramiento de psicólogos y abogados cuando la conducta dañina se haya producido.

Otra de las provincias que establece recaudos para el uso seguro de las NTIC es Salta. Allí se sancionó la ley 7933[14], que tiene como objetivo *"ayudar a prevenir riesgos y proteger los datos personales, la intimidad y la privacidad de las personas, en particular de niños y adolescentes"*. Dispone diversas situaciones de riesgo para los usuarios de las NTIC, entre ellas, las *"amenazas a la privacidad por robo, publicación y difusión de datos e imágenes personales en actitudes sexuales* 'sexting', *como así también la violación y deterioro de la identidad digital, que puede manifestarse a través de la facilitación de datos personales del menor, difusión por terceras personas de imágenes del menor sin su conocimiento, la grabación y difusión de imágenes inapropiadas por el menor"* [art. 2, inc. 5)].

La Provincia del Chaco tiene la ley 2634-E[15], que dispuso la creación del Programa de Contenidos y Estrategias sobre el Uso Seguro y Responsable de las Tecnologías de la Información y Comunicación para Menores. Su objetivo es idéntico al dispuesto en la norma salteña antes mencionada, y también prevé la misma disposición sobre el *sexting* [art. 2, inc. e)].

En países extranjeros como España se tipificó la nueva modalidad en la ley orgánica 1/2015, inciso 7) del artículo 197 del Código Penal español. En la norma se sanciona con prisión de tres meses a un año o una multa de seis a 12 meses al 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"*. Se establece la agravante si la divulgación de imágenes o videos la hace el cónyuge o un individuo que esté o haya estado

(13) BO: 17/7/2015
(14) BO: 15/7/2016
(15) BO: 17/7/2017

unida a la víctima por una relación de afectividad; no requiere que convivan o hayan convivido. También se eleva la pena cuando el delito se cometió con un fin lucrativo, la víctima es menor de edad o tiene discapacidad.

Distintos Estados de los Estados Unidos adoptaron medidas relacionadas con el fenómeno del *sexting* entre adolescentes. Los consideran delitos más leves que la pornografía o explotación infantil, y su sanción incluye penas de prisión y que el victimario sea registrado como delincuente sexual.(16)

El conflicto de la práctica surge cuando las imágenes o videos íntimos son publicados sin la debida autorización de los participantes. La conducta -propia de la esfera privada de los individuos- se puede convertir en *sextortion* en muchas ocasiones.

III - *SEXTORTION*

El paso siguiente al *sexting* deriva en la sextorsión (en castellano) o *sextortion* (en inglés). Consiste en la amenaza, chantaje o extorsión sexual que se le hace a la persona, previamente filmada o fotografiada desnuda o realizando actos sexuales en la intimidad, a cambio de dinero para no publicar las imágenes o videos. También para exigirle que entregue más fotografías de ella o de otra persona. Otra variante es que sea obligada a mantener relaciones sexuales. El agresor, al tener ese material, lo utiliza como un elemento de control sobre la víctima.

El Centro de Ciberseguridad(17) de la Ciudad Autónoma de Buenos Aires define a la sextorsión como la extorsión al dueño de una imagen y/o video con contenido erótico o sexual. El organismo es un centro de expertos en ciberseguridad, que ayuda y concientiza a los ciudadanos y al Gobierno de la Ciudad de Buenos Aires en los temas vinculados con la seguridad de la información.

En la Argentina, la nueva modalidad forma parte de la realidad social. Consecuentemente, es urgente establecer políticas públicas efectivas que utilicen mecanismos para evitarla y contrarrestarla. El doctor Daniel Monastersky -especialista en delitos informáticos- sostiene la importancia de denunciar este tipo de amenazas, en vez de pagarle al extorsionador.(18)

Durante el 2017, la Asociación Argentina de Lucha Contra el Cibercrimen (AALCC) denunció 39 casos, mientras que en 2016 solo en dos casos intervino la justicia(19). La organización contabilizó el asesoramiento de 140 víctimas de sextorsión en 2017, de las cuales la mitad se contactó con la asociación después de depositar el dinero.

En la Argentina, la conducta no está tipificada, pero sí está regulada la extorsión en el artículo 168 del Código Penal, el cual prevé una pena de prisión de cinco a diez años para el individuo que con *"intimidación o simulando autoridad pública o falsa orden de la misma, obligue a otro a entregar, enviar, depositar o poner a su disposición o a la de un tercero, cosas, dinero o documentos que produzcan efectos jurídicos"*. Se establece la misma

(16) Mendoza Calderón, Silvia: "El derecho penal frente a las formas de acoso a menores. *Bullying, ciberbullying, grooming y sexting*" - Ed. Tirant lo Blanch - España - 2013 - pág. 175

(17) Centro de Ciberseguridad de CABA: "Las mujeres y la ciberseguridad" - Boletín N° 35 - 8/3/2018

(18) "*Sextortion*, la nueva modalidad de chantaje: cómo proteger nuestros datos" - La Nación - 29/3/2018

(19) Druetta, Eugenio: "Sextorsión: denunciaron casi 20 veces más casos de chantaje por redes sociales" - Perfil - 13/12/2017

condena para la persona que utilice *"los mismos medios o con violencia, obligue a otro a suscribir o destruir documentos de obligación o de crédito".*

Tampoco la sextorsión está penada en las normas españolas. Solo en el artículo 243 el Código Penal español tipifica la extorsión, entendida como la acción que un individuo realiza para poder lucrar, obligando a otro mediante la violencia o intimidación a hacer u omitir un acto o negocio jurídico. Dicha situación menoscaba el patrimonio de la víctima o de un tercero. La escala penal para el delito es menor que la argentina: en el país europeo la pena privativa de la libertad es de uno a cinco años.

Para el abogado español Javier López, de acuerdo con los artículos 1275 y 1305 del Código Civil español que regulan el contrato de garantía "sexual", el cual tiene una causa ilícita que provoca su nulidad (STS del 2/12/1981, 28/9/2007 y 2/2/2012), podría esa conducta coincidir con la sextorsión. Considera que la *sextortion* se encuentra tipificada en los artículos 169, inciso 1), y 171, inciso 2), del Código Penal. Las penas de prisión son de hasta *"cinco años a quien amenace a otro con causarle un mal que constituya delitos contra la integridad moral, la libertad sexual, la intimidad o el honor; o a quien exija de otro una cantidad bajo la amenaza de revelar o difundir hechos referentes a su vida privada que no sean públicamente conocidos y puedan afectar a su fama, crédito o interés*".[20]

IV - *REVENGE PORN*

La pornovenganza o revenge porn implica *"la publicación no autorizada de imágenes o videos privados, generalmente contenido íntimo, por parte de una persona (generalmente, la expareja por sí o a través terceros) que lo hace por venganza luego de terminar la relación"*[21]. El vocablo se usó por primera vez en los Estados Unidos y se popularizó allí al aparecer en el sitio web *"Is anyone up?"*. La página difundía, sin autorización de las víctimas, imágenes de escenas íntimas de estas.

Durante el 2015, el Ministerio Público Fiscal de la Nación recibió consultas territoriales discriminadas por género, de las cuales el 70% corresponde a mujeres. La doctora Nora Cherñavsky sostiene que ese dato se eleva cuando las consultas son sobre extorsiones, acosos y publicaciones de imágenes íntimas no autorizadas.[22] La especialista relaciona esas conductas con la pornovenganza, producto de una ruptura de pareja. Agrega que la tecnología es el medio elegido para humillar a la víctima.

La Argentina no tiene tipificada la conducta. Los primeros casos de *revenge porn* se intentaron resolver en la justicia penal por la vía de los delitos de injurias y contra los derechos intelectuales[23]. Sin embargo, no se arribó a una solución judicial. Una propuesta ante la situación fue presentada en el Anteproyecto de Código Penal del año 2014[24], presidido por el exjuez de la Corte Suprema de la Nación, Eugenio R. Zaffaroni. El artículo 120 del Anteproyecto establecía una pena de prisión de seis meses a dos

(20) López, Javier: "Ciberdelitos sexuales" - Revista Byte - España - 14/7/2017

(21) Palazzi, Pablo A.: "Difusión no autorizada de imágenes íntimas (*revenge porn*)" - ED - 2/3/2016 - Nº 13906 - año LIV

(22) Centro de Ciberseguridad de CABA: "Las mujeres y la ciberseguridad" - Boletín N° 35 - 8/3/2018

(23) Palazzi, Pablo A.: "Difusión no autorizada de imágenes íntimas (*revenge porn*)" - ED - 2/3/2016 - Nº 13906 - año LIV

(24) La Comisión para la elaboración del proyecto de ley de reforma, actualización e integración del Código Penal de la Nación fue dispuesta por el dec. (PEN) 678/2012

años y una multa de diez a ciento cincuenta días, para el individuo que *"vulnerare la privacidad de otro, mediante la utilización de artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o imagen, o se apoderare de registros no destinados a la publicidad"*.[25]

En cuanto a la legislación argentina, se presentó el Proyecto de Ley S-2119/16 -anteriormente mencionada-, que tuvo media sanción en Senadores. El artículo 155 bis que se propone introducir al Código penal se ubica en el Título V entre los "Delitos contra la libertad", Capítulo III: "Violación de secretos y de la privacidad". La ubicación permite inferir que el bien jurídico protegido por la infracción es el derecho a la intimidad, que incluye la vida sexual de la persona. Los fundamentos del Proyecto se dirigen a los casos de "pornografía de venganza" y los define como un problema de dimensiones globales. Además, las autoras del Proyecto sostienen que las NTIC y los dispositivos electrónicos para la producción de material audiovisual favorecen *"el uso de nuevas prácticas y conductas en los espacios de la intimidad sexual, de las que resultan imágenes o videos que son el resultado de un acuerdo entre las partes involucradas pero reducidas al espacio de confianza/privacidad en que fueron obtenidas"*. Hacen hincapié en los supuestos en que *"por represalia, resentimiento, extorsión, venganza o sentimientos de animosidad respecto de sus exparejas o relaciones ocasionales de intimidad"*, suben al ciberespacio imágenes y/o videos que afectan la privacidad, la libertad y dignidad de las personas.

El especialista en delitos informáticos Pablo Palazzi[26] considera que la figura de *revenge porn* está tipificada en el artículo 197, inciso 7), del Código Penal español, mencionado en el punto II del presente artículo.

En los Estados Unidos, la Universidad de Michigan determinó que en el 90% de los casos de "pornovenganza" el agresor es un hombre y que cinco de cada diez víctimas admiten haber recibido fuertes insultos en las redes[27]. Más de 40 Estados americanos sancionaron leyes que penan el *revenge porn*[28]. La vicepresidente de *Cyber Civil Rights Initiative,* la abogada Mary A. Franks, impulsó desde la organización sin fines de lucro el reclamo para combatir los abusos online. La profesora de Derecho Penal de la Universidad de Miami sostiene que existen 3.000 sitios web que publican pornografía de venganza, la cual es redistribuida a través de los medios digitales.

V - *STALKING*

El *stalking* es un término de origen anglosajón que se traduce al castellano como acoso o acecho. La conducta del *stalker* es descripta como hostigamiento, persecución, acecho, acoso para la víctima. Los *stalkers* siguen a sus víctimas continuamente, solo observándolas o también ingresando a su ámbito laboral o familiar. Es considerado un fenómeno socialmente relevante, aunque complejo de tipificar.[29]

(25) Palazzi, Pablo A.: "Difusión no autorizada de imágenes íntimas *(revenge porn)*" - ED - 2/3/2016 - Nº 13906 - año LIV

(26) Palazzi, Pablo A.: "Difusión no autorizada de imágenes íntimas *(revenge porn)*" - ED - 2/3/2016 - Nº 13906 - año LIV

(27) "Pornovenganza: cada vez más gente revela en la web intimidades *hot* de sus ex" - Clarín - 14/9/2014

(28) Cyber Civil Rights Initiative: "40 states + DC have revenge porn laws"

(29) Manso Porto, Teresa: "Agresiones a bienes altamente personales a través de las TICs en menores y redes sociales", en Cuerda Arnau, María L. (Dir.) - Ed. Tirant lo Blanch - España - 2016 - pág. 311

La primera vez que se reguló el ciberacoso fue en la legislación penal del Estado de California en los años 90, luego del asesinato de la actriz Rebecca Schaeffer[30]. Actualmente, la regulación se extendió a todos los Estados de la Unión y se lo estableció como delito federal. Texas promulgó el *Stalking by Electronic Communications Act,* en 2001, y dos años después Florida, a través de la HB 479, prohibió la conducta. Por su parte, el Estado de *"Missouri revisó sus estatutos sobre acoso para incluir el acoso y el acecho mediante comunicaciones electrónicas y telefónicas, así como el ciberacoso escolar después del suicidio de Megan Meier en 2006".*[31]

Recientemente en España, mediante la ley orgánica 1/2015 que modificó el Código Penal, se introdujo la figura en los artículos 172 ter y 173, inciso 2). Diversas conductas son descriptas en la primera norma, que sanciona con prisión de tres meses a dos años o multa de seis a veinticuatro meses. Los hechos descritos en el artículo son perseguibles si la víctima o su representante legal hacen la denuncia. Establece que el *stalker* acosa a una persona de manera insistente y reiterada, sin estar legítimamente autorizada alguna de las conductas siguientes, y modifica de forma grave el desarrollo de su vida cotidiana:

> *"1. la vigile, persiga o busque su cercanía física;*
>
> *2. establezca o intente establecer contacto con ella a través de cualquier medio de comunicación o por medio de terceras personas;*
>
> *3. mediante el uso indebido de sus datos personales, adquiera productos o mercancías o contrate servicios, o haga que terceras personas se pongan en contacto con ella;*
>
> *4. atente contra su libertad o contra su patrimonio, o contra la libertad o patrimonio de otra persona próxima a ella".*

La pena será de prisión de seis meses a dos años si se afecta a una persona vulnerable por su edad, enfermedad o situación. Las sanciones del artículo se imponen independientemente de las que puedan corresponder a los delitos en que se hubieran concretado los actos de acoso.

La norma hace especial atención a la situación en que el agraviado es alguna de las personas mencionadas en el inciso 2) del artículo 173; en esos casos se impondrá una pena de prisión de uno a dos años, o trabajos en beneficio de la comunidad de sesenta a ciento veinte días. Y la denuncia no deberá hacerla el afectado o su representante legal.

Todavía en la Argentina el *stalking* no está tipificado, aunque el avance de la era digital lleva a presentar proyectos de ley, como el S-4136/2016[32]. Propone la incorporación del artículo 149 quater al Capítulo I del Título V del Código Penal: *"Será reprimido con prisión o reclusión de seis meses a tres años el que en forma reiterada y sin estar legítimamente autorizado ejecute un patrón de conducta destinado a entrometerse en la vida del otro y alterar su vida cotidiana. Se considerarán conductas de acoso: 1. Vigilar, perseguir*

(30) Aboso, Gustavo E.: "*Stalking* y *cyberstalking*: El dominio de la víctima mediante terror psicológico como nueva expresión de atentado contra la libertad personal" - El Dial - 31/5/2016

(31) Galeazzo, Florencia: "Efectos del acoso escolar, cyberbullying y grooming en la responsabilidad parental" - ERREIUS - Temas de Derecho de Familia, Sucesiones y Bioética - octubre/2017 - Cita digital IUSDC285472A

(32) Archivado el 25/4/2018

o buscar la cercanía física de otro. 2. Establecer o intentar establecer de forma insistente contacto con otro a través de cualquier medio de comunicación, o por medio de terceras personas. 3. Utilizar indebidamente datos personales de otro para adquirir productos o mercancías, o contratar servicios, o hacer que terceras personas se pongan en contacto con otro. La pena será de uno a cuatro años si se trata de hechos constitutivos de violencia de género o ejecutados en perjuicio de una persona especialmente vulnerable por razón de su edad o enfermedad".

En los fundamentos se sostiene que el derecho de privacidad y libertad es y debe ser un punto de gran resguardo y cuidado. Agrega que de esa manera se respetaría lo estipulado por la Constitución Nacional y los tratados internacionales.

VI - CONCLUSIÓN

La era de la tecnología presenta un panorama distinto al tradicional; allí el ciberespacio toma protagonismo. *"Internet es una red informática, tecnológica, pero también de subjetividades, un espacio en donde las emociones se encuentran, se entretejen, se expresan, se contienen y se liberan"*[33]. Las personas en sus casas, o donde gusten, pueden generar contenido y hacerlo público. Como plantea el filósofo Byung-Chul Han: *"Hoy ya no somos meros receptores y consumidores pasivos de informaciones, sino emisores y productores activos ... esta doble función incrementa enormemente la cantidad de información. El medio digital no solo ofrece ventanas para la visión pasiva, sino también puertas a través de las cuales llevamos fuera las informaciones producidas por nosotros mismos".*[34]

Por consiguiente, ante la masiva producción de contenidos, que egresan de la esfera privada -sin consentimiento- y dañan, aparece la imperiosa necesidad de sancionar nuevos tipos penales vinculados a los medios digitales y de índole sexual, acompañados con políticas de concientización y mecanismos de prevención. Porque, pese a ser los delitos sexuales muy antiguos, evolucionan como lo hacen los individuos y las sociedades.

Sin embargo, el respeto por el principio constitucional de legalidad debe primar (art. 18, CN), en tanto no hay crimen ni pena sin ley que previamente lo haya contemplado. Por tal motivo, hay sobrados proyectos, como los mencionados *supra*, que se ajustan a la ciberrealidad, lo cual conduce a que se haga justicia y, de algún modo, se repare a la víctima.

(33) Ennis, Victoria y Maya, Marian: "Los fantasmas del Facebook" - Anfibia: Crónicas y Ensayos/1 - Alarcón, Cristian (Dir.) - 1ª ed. - Ed. UNSAM Edita - Bs. As. - abril/2015 - pág. 51

(34) Byung-Chul Han: "En el enjambre" - Herder Editorial - Barcelona - 2014 - pág. 22

Reflexiones sobre el acceso ilegítimo a un sistema o dato informático

María M. Roibón(*)

I - INTRODUCCIÓN: ANTECEDENTES LEGISLATIVOS DE LOS DELITOS INFORMÁTICOS EN LA ARGENTINA

La delincuencia informática comprende un amplio espectro de actividades ilícitas que tienen en común el medio electrónico en el que tienen lugar o del que se valen. En ese sentido, se definen a los delitos informáticos como *"aquellas conductas disvaliosas socialmente y reprochables desde el punto de vista penal, que, concretadas mediante instrumentos y sistemas informáticos y virtuales, pueden tener como objeto la violación de cualquiera de los bienes jurídicos tutelados por la ley, en un momento dado*".(1)

El 4/6/2008, con la sanción de la ley 26388 se reformó el Código Penal argentino, modificándose ciertos aspectos de los delitos existentes para dar cabida al uso ilícito de las nuevas tecnologías en la afectación de bienes jurídicos ya tutelados. Su texto tipifica como delitos informáticos: la pornografía infantil por internet u otros medios electrónicos (art. 128, CP); el acceso no autorizado a un sistema o dato informático de acceso restringido (art. 153 bis, CP); la violación de las comunicaciones electrónicas sin la debida autorización, su revelación indebida o la inserción de datos falsos (arts. 155 y 157 bis, CP), el fraude informático (art. 173, CP); el daño o sabotaje informático (arts. 183 y 184, CP) y los delitos contra las comunicaciones (art. 197, CP).

(*) Abogada (UCA - Rosario). Empleada de la Fiscalía Federal N° 1 de Rosario. Exabogada de la Dirección Regional Rosario II de la AFIP-DGI, a la que ingresó mediante concurso

(1) Zarich, Faustina: "Derecho informático" - Ed. Juris - Rosario - T. 4 - pág. 134

La ley 26388 se basó en las disposiciones de la "Convención sobre el Cibercrimen", más conocida como el Convenio de Budapest, del 23/11/2001 del que la Argentina forma parte junto con otros países como Estados Unidos, Italia, España, Japón, Canadá, Israel, Chile, República Dominicana y Panamá. Este convenio es el único tratado internacional sobre delitos informáticos y obtención de evidencia digital. Tratado que además propone la integración (u homogeneización) de normas procesales e investigación cooperativa de conductas ilícitas en internet. Los principales temas que contempla la Convención son el acceso ilícito a la información y la interferencia en el acceso a ella, la seguridad de los sistemas y de la red, la falsificación informática, el fraude informático, la pornografía infantil y los delitos de derechos de autor.

El 13/11/2013 se sancionó en nuestro país la ley 26904, la que incorporó el delito de *grooming* al derecho interno argentino. Es así que estableció como artículo 131 del Código Penal el siguiente: "*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*".

Finalmente, la ley 27436 -sancionada el 21/3/2018- sustituyó el artículo 128 del Código Penal argentino, penando la simple tenencia de pornografía infantil. Antes se sancionaba la tenencia de ese material solo si tenía fines de distribución o comercialización.

II - PARTICULARIDADES DE LOS DELITOS INFORMÁTICOS

El modo de comisión de los delitos informáticos les otorga ciertas particularidades que los diferencian instrumentalmente del resto haciendo que su investigación (policial y judicial) resulte mucho más compleja que en otros casos. Además, el medio a través del cual se consuman estos ilícitos permite una gran variedad de posibilidades (que incluyen amenazas, violación a la intimidad, relevación de secretos, prostitución, corrupción de menores, exhibicionismo, etc.). Estas nuevas acciones lesionan tanto a las personas como a sus bienes.

Esas peculiares características son -utilizando como referencia en forma parcial al Dr. Daniel Hargain- las siguientes:

1. En primer lugar, la potencialidad del alcance de las conductas desarrolladas a través de internet, que no se circunscriben a un ámbito geográfico determinado, sino que pueden esparcirse a través de toda la web, que hace que estos crímenes no reconozcan fronteras territoriales. En su mayoría, se trata de delitos trasnacionales, como las redes de pedofilia o de lavado de dinero.
2. En segundo lugar, el anonimato. En muchísimas ocasiones resulta imposible o muy difícil identificar a quién está detrás de una computadora, desde dónde se envía un mensaje a través de la red o al responsable de una página web.
3. Y, en tercer lugar, la complejidad técnica del tema y el dinamismo vertiginoso con que evoluciona. El punto más dramático, a mi entender, para la persecución penal de los mismos.[2]

(2) Hargain, Daniel: "Incidencia del comercio electrónico en el ámbito jurídico: planteo general" en Comercio electrónico. Análisis jurídico multidisciplinario - Euro Editores SRL - Bs. As. - 2003 - págs. 22/3

Igualmente, Fernando Tomeo sostiene lo siguiente: "*Esta nueva realidad 2.0 fue bien recibida por los cibercriminales, que cuentan con múltiples herramientas tecnológicas para infringir la ley; no por casualidad muchos consideran que el cibercrimen constituye una actividad más rentable que el narcotráfico. La tecnología los invita a cometer cibercrímenes, donde se delinque con armas mucho más eficaces que las tradicionales, dado que a simple vista no parecen armas; son gratuitas. Además, cuentan con adicionales claves como el anonimato, la difícil persecución y en varios casos corren con la ventaja de que aún no existen leyes que tipifiquen sus conductas dolosas en la web*".(3)

En síntesis, de la combinación de estas singularidades (posibilidades de acceso y alcance casi ilimitadas, anonimato, sofisticación tecnológica y cambios constantes) se derivan enormes dificultades para que el legislador y la justicia puedan dar una respuesta adecuada a este fenómeno. De ahí, la necesidad de contar con instrumentos de cooperación y coordinación internacionales eficaces que posibiliten llevar a cabo investigaciones eficaces, rápidas, coordinadas y la preservación de los elementos de prueba en procesos, cuyas evidencias resultan frágiles y volátiles; así como la sanción de nuevos tipos penales que se adecuen a los desafíos que plantean las nuevas tecnologías y la sociedad de la información.

III - EL ACCESO ILEGÍTIMO A UN DATO O SISTEMA INFORMÁTICO EN EL CONVENIO SOBRE CIBERCRIMINALIDAD DE BUDAPEST

Los doctores Ricardo Gutiérrez, Laura C. Radesca y Marcelo A. Riquert entienden que la reforma introducida por ley 26388, en general, sirvió no solo para actualizar el Código, sino para acercar nuestra legislación interna a las demandas del Convenio sobre Cibercriminalidad de Budapest (2001) en materia fondal. En ese sentido, expresan que la redacción del artículo 153 bis permite cubrir la tipicidad reclamada por el artículo 2 del Tratado, el que establece que "*las partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, el acceso doloso y sin autorización a todo o parte de un sistema informático. Las partes podrán exigir que la infracción sea cometida con vulneración de medidas de seguridad, con la intención de obtener los datos informáticos o contra intención delictiva, o también podrán requerir que la infracción se perpetre en un sistema informático conectado a otro sistema informático*".

Los profesionales citados reflexionan que "*es interesante resaltar que si bien el Convenio toma partido por considerar delito el simple* hacking*, permite que los signatarios introduzcan condicionantes tales como la vulneración de medidas de seguridad y elementos subjetivos distintos del dolo como la intención de obtener datos u otra intención delictiva. También permite que la tipificación se limite a casos de acceso a sistema informático que esté conectado a otro*".(4)

(3) Tomeo, Fernando: "Redes sociales y tecnología 2.0" - Ed. Astrea - Bs. As. - 2014 - pág. 206

(4) Gutiérrez, Ricardo; Radesca, Laura C. y Riquert, Marcelo A.: "Código Penal Comentado" - Revista Pensamiento Penal - consultado el 19/5/2018

IV - EL DELITO DEL ACCESO ILEGÍTIMO A UN SISTEMA O DATO INFORMÁTICO EN LA LEGISLACIÓN ARGENTINA

El acceso ilegítimo a un sistema o dato informático se encuentra previsto en el artículo 153 bis del Código Penal, el que dispone que "*será reprimido con prisión de quince días a seis meses, si no resultare un delito más severamente penado, el que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido. La pena será de un mes a un año de prisión cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros*".

Pablo A. Palazzi señala que "*mediante el artículo 153 bis del Código Penal se ampara la reserva, la confidencialidad y el derecho a la privacidad del titular del sistema y del dato informático. Este puede ser tanto una persona natural como una jurídica. Ello puede resultar difícil de comprender cuando se trate de la segunda ... Pero cabe recordar que estas también tienen un derecho a la reserva y al secreto de sus papeles privados, y hoy en día esos papeles están almacenados en su gran mayoría en ordenadores, por lo que las prohibiciones de acceso tienden a amparar estos registros informáticos*".[5]

Conviene aclarar que el valor confidencial del dato o sistema informático al que se refiere la norma citada no significa "personal", aunque ambos atañan a la privacidad. El Código Penal argentino sanciona dos figuras de acceso ilegítimo: el indebido o no autorizado a sistemas informáticos (art. 153 bis) y la prohibición de acceso ilegítimo a banco de datos personales (art. 157 bis).

V - ¿QUÉ ES EL *HACKING*?

La figura penal tipificada por el artículo 153 bis del Código Penal comprende lo que se conoce como "*hacking*" o intrusismo informático. El tipo penal supone la comisión de una conducta de acceso y/o permanencia no autorizada o indebida a sistemas informáticos, una interferencia en redes de comunicación electrónicas protegidas.

El doctor Tomeo explica que "*la actividad de los grupos* hackers *comenzó a principios de la década de los ochenta, con la aparición de las computadoras domésticas, y la palabra* hacking *empezó a utilizarse para referirse a personas que encontraban soluciones no convencionales a las fallas que presentaban los diseños originales de los programas informáticos*".

Generalmente, estas habilidades eran asociadas a estudiantes que desmenuzaban los programas para que pudieran funcionar de manera correcta, y la palabra, en ese contexto, era concebida como un halago. Pero con el correr de los años, estas prácticas evolucionaron, hasta constituir lo que Jorge Vega Iracelay de Microsoft considera como un crimen organizado.

Pero si bien, actualmente, el término "*hacker*" se asocia generalmente a los criminales informáticos; con el desarrollo de la comunidad virtual, podemos distinguir grupos con objetivos variados:

(5) Palazzi, Pablo A.: "Los delitos informáticos en el Código Penal. Análisis de la ley 26388" - Ed. AbeledoPerrot - Bs. As. - 2009 - págs. 101/2

a) *Black hats*: es el grupo principal. Básicamente, suelen practicar actividades ilícitas con fines lucrativos. Pueden, por ejemplo, romper sistemas de seguridad de computadoras, realizar entradas remotas no autorizadas, colapsar servidores, entrar a zonas restringidas, infectar redes o apoderarse de ellas, entre otras.

b) *White hats*: también son llamados *hackers* éticos. Generalmente, son personas que trabajan para empresas de informática, protegiendo y reparando errores en los sistemas.

c) *Blue hats*: trabajan en un ordenador oficial o en una empresa de seguridad que intenta descifrar los problemas potencialmente explotables.

d) *Script-kiddies*: carecen de experiencia y ejercen formas básicas de *hacking*; por ejemplo, buscan y descargan programas y herramientas de intrusión informática, para luego ejecutarlos como simple usuario, sin preocuparse del funcionamiento interno de estos ni de los sistemas sobre los que funcionan.

e) Hacktivistas: los motivos por los cuales hackean se asocian a movimientos ideológicos concretos, relacionados con alguna causa social, promoviendo cambios en los modos de vida, libertad del conocimiento y la justicia social.

f) *Hackers* de élite: pertenecen a uno o varios colectivos virtuales oscuros y prestigiosos y se consideran los más expertos de todos.(6)

VI - GNOSEOLOGÍA DEL TIPO PENAL

1. Acción típica

La acción típica del delito bajo análisis consiste en "*acceder en forma indebida o no autorizada, o excediendo una autorización concedida, a un sistema de tratamiento automatizado de la información de acceso restringido. La conducta típica es acceder, esto es ingresar, penetrar, en forma indebida o no autorizada, o excediendo una autorización conferida, a un sistema o dato informático. Debe tratarse de un sistema o dato informático de acceso restringido, vale decir, privado, no abierto al público en general, como lo son algunas redes o sitios de internet. Si el acceso se produce con el consentimiento o permiso del titular de la red, sitio, correo electrónico, etc., la conducta es atípica*".(7)

Los incisos a) y b) del artículo 1 del Convenio sobre Cibercriminalidad (2001) definen las expresiones "sistema informático" y "dato informático" de la siguiente manera: "*A los efectos del presente Convenio, la expresión: a) 'sistema informático' designa todo dispositivo aislado o conjunto de dispositivos interconectados o unidos, que aseguran, en ejecución de un programa, el tratamiento automatizado de datos; b) 'datos informáticos' designa toda representación de hechos, informaciones o conceptos expresados bajo una forma que se preste a tratamiento informático, incluido un programa destinado a hacer que un sistema informático ejecute una función*".

(6) Tomeo, Fernando: "Redes sociales y tecnología 2.0" - Ed. Astrea - Bs. As. - 2014 - págs. 210/11

(7) Buompadre, Jorge E.: "Manual de derecho penal. Parte especial" - Ed. Astrea - Bs. As. - 2017 - pág. 371

Palazzi entiende por "*sistema o dato informático de acceso restringido*" aquel "*que tiene alguna medida de seguridad que impida el libre ingreso*". Es decir que el texto legal no "*prohíbe acceder a sistemas o redes abiertas, o al contenido publicado en un sitio de internet de acceso público (como lo son la gran mayoría) ... si es un dato o sistema de libre acceso, no habrá delito ... El sistema o dato informático de acceso restringido es un ordenador o un conjunto de informaciones que no se encuentran fácilmente accesibles porque no están conectados a una red, o porque se hallan amparados con una clave de ingreso*".(8)

Por lo tanto, la acción que se penaliza es la entrada por cualquier medio a un ordenador o sistema informático extraño o ajeno. Esto puede realizarse de diferentes maneras, ya sea en forma remota. Por ejemplo, con una clave de acceso no permitida o sustraída: utilizando los datos concernientes al sujeto pasivo, o sea como si fuera en realidad el legítimo usuario del sistema.

También puede accederse a un sistema informático ajeno mediante la instalación de un programa espía o *spyware*, el que se instala sin el permiso del titular. A través de estos programas se recopila información de un ordenador. Información que luego se trasmite a una entidad externa sin el conocimiento o el consentimiento del propietario del ordenador. Estos programas de espionaje pueden instalarse, sin que el propietario del sistema informático lo sepa, ya sea porque se distribuyen en un programa, sin advertirle al usuario del sistema informático que ese programa puede acceder a donde no debía. Asimismo, el *spyware* también puede instalarse en un sistema informático mediante un virus: un troyano que se distribuye por correo electrónico, y que termina siendo ejecutado -por error o desconocimiento- por el usuario del ordenador.

Pero el acceso indebido no necesariamente se realiza en forma remota, también puede darse el supuesto de que el autor del delito lo haga simplemente leyendo el contenido de la pantalla de la computadora -sin el permiso del titular de la misma- o copiando archivos para acceder posteriormente al contenido del sistema informático. Pero como sostiene Palazzi este ilícito "*no requiere ninguna acción adicional (por ejemplo, copia o borrado o reenvío de datos), es decir, se consuma por el mero acto, con independencia de que luego se cometan otros delitos*". Se trata -para el autor- "*de una figura de peligro*".(9)

Igualmente, el acceso ilegítimo puede efectuarse, aprovechando las deficiencias de los procedimientos de seguridad del sistema o en alguno de sus procedimientos o usar un programa desencriptador.

2. Sujetos del delito

Buompadre expresa que el sujeto activo "*puede ser cualquier persona, sin importar el sexo ni la edad, ni el nivel de conocimiento informático que posea. Sujeto pasivo es el titular del sistema o dato informático violado*".(10)

Si bien el sujeto activo puede ser cualquiera, entiendo que, por tratarse de un delito vinculado a la tecnología, se requieren ciertos conocimientos mínimos para que pueda serle imputable el tipo objetivo como obra propia.

(8) Palazzi, Pablo A.: "Los delitos informáticos en el Código Penal. Análisis de la ley 26388" - Ed. AbeledoPerrot - Bs. As. - 2009 - págs. 102/3

(9) Palazzi, Pablo A.: "Los delitos informáticos en el Código Penal. Análisis de la ley 26388" - Ed. AbeledoPerrot - Bs. As. - 2009 - pág. 104

(10) Buompadre, Jorge E.: "Manual de derecho penal. Parte especial" - Ed. Astrea - Bs. As. - 2017 - pág. 372

En este punto, conviene señalar que el "*ethical hacking*" (la ciencia que tiene por objeto el testeo de computadoras y redes para encontrar vulnerabilidades de seguridad y modificar esas fallas antes de que sean explotadas ilegalmente) queda fuera del ámbito típico de la norma. En muchos de estos casos, el acceso a las redes y sistemas ajenos se hace con finalidades académicas o empresarias, siendo que el acceso ocurre con el consentimiento del dueño o del titular de la red que está siendo testeada. Por último, resta decir que sobre este tema se ha escrito muchísimo, por lo que su tratamiento en profundidad excede con creces el objetivo del presente trabajo.

3. Tipo subjetivo

Es un tipo doloso de dolo directo, que excluye el dolo eventual. El dolo consiste en la voluntad de "*intromisión o ingreso al sistema o dato informático restringido, con el conocimiento que el acto es ilegítimo*". Es decir que carece de derecho, permiso, autorización o consentimiento para hacerlo.

El primer párrafo consagra la punición como conducta básica de quien con conocimiento y sin autorización, o excediéndola, accede por cualquier medio a un sistema o dato informático de acceso restringido, deja fuera por medio de este requerimiento cognitivo ("a sabiendas") la punición de acceso fortuito, casual o imprudente. El tipo no requiere elementos subjetivos distintos del dolo, esto es, de tendencia interna o trascedente (ultrafinalidad usualmente destacada con la preposición "para" o "con el fin de") o peculiar o con cierto ánimo. Por ello, cualquier otra finalidad que la descripta sería propia de algún delito más grave y por esta razón se ha caracterizado al sujeto activo como el autor que procura eliminar los pasos de seguridad del sistema para ver el contenido de la información protegida.

El error sobre un elemento del tipo objetivo excluye el dolo y la responsabilidad penal tanto si es invencible como vencible, dado que no se encuentra previsto el tipo culposo.(11)

4. Subsidiaridad

El artículo 153 bis establece que resultará de aplicación este ilícito "*si no resultare un delito más severamente penado*". En general, el ingreso indebido a un sistema informático ajeno integra la tipicidad de la acción de otros delitos más graves como la estafa, el daño o el sabotaje informático. En estos casos, se descarta la aplicación del artículo mencionado siendo desplazado por la norma de mayor punibilidad.

Gutiérrez, Radesca y Riquert manifiestan que a este ilícito se lo caracteriza como delito "*de antesala o delito barrera u obstáculo en virtud de que se trata de una figura que opera subsidiariamente cuando no se puede acreditar la realización de otra más grave como la alteración o supresión de datos. Sin embargo, corresponde tener presente que, por lo general, los* **hackers** *evitan que su acceso ilegítimo sea descubierto y, por lo tanto, no destruyen datos ni dañan o alteran el sistema, en procura de que su presencia no llame la atención del administrador o usuario del caso*".(12)

(11) Gutiérrez, Ricardo; Radesca, Laura C. y Riquert, Marcelo A.: "Código Penal Comentado" - Revista Pensamiento Penal - consultado el 19/5/2018

(12) Gutiérrez, Ricardo; Radesca, Laura C. y Riquert, Marcelo A.: "Código Penal Comentado - Revista Pensamiento Penal - consultado el 19/5/2018

5. Agravantes

El artículo 153 bis, segundo párrafo, del Código Penal establece lo siguiente: "*La pena será de un (1) mes a un (1) año de prisión cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros*".

En estos casos, la pena se duplica, porque se considera que estos supuestos (bienes o servicios públicos) requieren una protección especial. En este sentido, señala Palazzi que la *"ley hace referencia a un organismo público estatal, porque la idea fue dejar de lado a los organismos no estatales, aunque fueren públicos (por ejemplo, el Colegio de Abogados de la Capital Federal)".*

El autor citado agrega: "*la otra agravante consiste en el acceso a un proveedor de servicios públicos o financieros. Aunque la ley es muy general, el término proveedor de ... de servicios financieros*" es más amplio que el de entidad financiera (art. 2, L. 21526), pudiendo incluir un agente de bolsa, una casa de cambios o un medio de pago *online* o de recaudación de pagos. Seguramente en estos casos el acceso será la antesala de una estafa o hurto informático. Con esta agravante, el legislador quiso amparar los sistemas informáticos que estén relacionados con las finanzas y el dinero, dado que serán probablemente los más atacados por los intereses económicos que existen detrás de ellos.(13)

Buompadre opina que "*el fundamento de la mayor penalidad reside en la naturaleza de los organismos protegidos, que deben ser públicos (organismos del Estado, nacional, provincial o sus entes descentralizados o autárquicos) o en el servicio público que prestan. La mayor penalidad no obedece al hecho de brindar más protección a las actividades que realizan estas entidades, sino al peligro de que a través del acceso no autorizado se obtengan grandes cantidades de información que resulte altamente sensible para los usuarios de productos bancarios (por ejemplo, domicilios, claves de usuarios, niveles de ingresos, sueldos)*".(14)

VII - LA COMPETENCIA FEDERAL PARA INVESTIGAR EL DELITO DEL ARTÍCULO 153 BIS DEL CÓDIGO PENAL

En los autos caratulados "N. N. s/violación sist. informático art. 153 bis 1° párrafo" (Competencia CSJ 5901/2014/CS1), el 23/6/2015, el procurador fiscal determinó, en una contienda negativa de competencia entre el Juzgado en lo Penal, Contravencional de Faltas N° 29 de la Ciudad Autónoma de Buenos Aires y el Juzgado Nacional en lo Criminal y Correccional Federal N° 12, que en la causa debía intervenir la justicia federal. La Corte Suprema de Justicia de la Nación adhirió al dictamen del procurador.

En los autos citados, Daniela Marlene O. denunció haber recibido continuamente mensajes ofensivos en Facebook en contra de ella o su pareja y que alguien ingresó ilegítimamente en su cuenta de esa red social, desde donde se enviaron mensajes y fotos a sus contactos. Además, que se creó una cuenta utilizando su identidad y fotografía, y que se habrían robado archivos de su ordenador.

(13) Palazzi, Pablo A.: "Los delitos informáticos en el Código Penal. Análisis de la ley 26388" - Ed. AbeledoPerrot - Bs. As. - 2009 - págs. 116/17

(14) Buompadre, Jorge E.: "Manual de derecho penal. Parte especial" - Ed. Astrea - Bs. As. - 2017 - pág. 372

La jueza local encuadró los hechos en el delito previsto en el artículo 153 bis y declinó competencia a favor de la justicia federal por considerar que el ingreso ilegal a una cuenta de Facebook es asimilable a un hecho de violación de correspondencia.

El juzgado federal no aceptó tal atribución con fundamento en el criterio general de actuación, según la cual el delito en cuestión debe ser investigado por los jueces locales, y por considerar que los hechos denunciados no afectaron una institución federal ni vulneraron intereses nacionales.

Vuelto el legajo al tribunal de origen, su titular insistió con su criterio, dio por trababa la contienda y lo elevó a la Corte.

Toda vez que no existió controversia acerca de la calificación legal de los hechos, el procurador Eduardo E. Casal entendió que al caso resultaba aplicable la doctrina "*según la cual el acceso ilegítimo a una comunicación electrónica o dato informático de acceso restringido, en los términos de los artículos 153 y 153 bis, según la ley 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 (arts. 2 y 3, L. 19798), debe ser investigado por la justicia federal (conf. competencia N° 778, L. XLIX,* in re 'D., S. D. s/violación correspondencia medios electrónicos - art. 153 2º p.*', resuelta el 24/6/2014)*".

VIII - VALORACIÓN DEL DICTAMEN DEL PROCURADOR FISCAL

Estimo que debería revisarse este criterio jurisprudencial, ya que el bien jurídico que suscita la competencia federal en lo penal es el daño o perjuicio ocasionado a los intereses del Estado nacional, así como a su patrimonio. Es decir que si el ingreso ilegítimo a un sistema restringido afecta la privacidad y la confidencialidad de un particular -sin que se afecten ni comprometan el orden económico y financiero del Estado Nacional, ni los bienes ni la rentas ni los intereses ni las instituciones de la Nación ni la soberanía nacional (conf. los lineamientos de la L. 48, los arts. 75 y 116, CN y 33, CPPN), corresponde que intervenga la justicia ordinaria con competencia penal.

Siendo por lo demás disputable, por un lado, que en todos los casos el acceso a un sistema o dato informático se haga necesariamente a través de un servicio de telecomunicaciones en los términos de la ley 19798 y, por otro, que cuando se trate de un suceso singular -como seguramente ocurrirá en muchas ocasiones- pueda predicarse de él que afecta tales servicios de telecomunicaciones "*de interés de la Nación*", es decir que perjudique la generalidad de las comunicaciones por importar una interrupción o entorpecimiento del servicio mismo.

Curiosa e inconsistentemente así lo tenía decidido la CSJN en casos sustancialmente análogos; entre otros:

> "*Es competente la justicia contravencional que previno para continuar con la investigación de los hechos -adquisición de un software para manipular computadoras de forma remota y despliegue de maniobras para atacar el sitio web de la denunciante enmarcados en los supuestos de daño informático, previsto y reprimido en el artículo 183, segundo párrafo, del Código Penal*". (Del dictamen de la Procuración General al que la Corte remite; Competencia CSJ 2358/2014/CS1 "Russo, Christian Carlos y otro s/infracción art. 183 del Código Penal - incidente de competencia" - 23/6/2015).

"*Debe intervenir la justicia provincial -y no la contravencional- en cuyo ámbito se habría realizado la conexión de internet al momento de difundir -mediante una dirección de correo electrónico- las imágenes de pornografía infantil toda vez que la competencia penal en razón del territorio se establece atendiendo al lugar donde se ha consumado el delito (Fallos: 330:2954)*". (Del dictamen de la Procuración General al que la Corte remite; Competencia CSJ 5685/2014/CS1 "Sequiera, Nicolás s/publicaciones, reprod. y/o distrib. obscenas" - 30/6/2015).

Sin descuidar desde una perspectiva quizás pragmática pero atendible por su trascendencia que, con el irrestricto criterio de la anterior cita jurisprudencial podrían sin más resultar de competencia federal todos los delitos cometidos a través de la web; sin duda la violación de las comunicaciones electrónicas sin la debida autorización, su revelación indebida o la inserción de datos falsos (arts. 155 y 157 bis, CP); el fraude informático (art. 173, CP); el daño o sabotaje informático (arts. 183 y 184, CP), lo que conduciría a atiborrar al fuero federal contribuyendo al colapso que atraviesa en la actualidad la justicia federal con competencia penal.

Finalmente, no se puede prescindir de considerar sistemáticamente que el delito de que se trata es de acción privada (art. 73, CP), lo que importa es que para el legislador se trata de un delito que, por no considerarse de una gravedad tal que afecte al orden público de la sociedad, que es casi como decir el interés de la Nación, no puede ser perseguido de oficio por los poderes públicos.

IX - REFLEXIONES FINALES

El derecho internacional viene exhortando a los estados a perseguir el intrusismo informático como una modalidad por sí sola de carácter criminal. Así, el citado Convenio sobre la Ciberdelincuencia de Budapest de 23/11/2001, ya reseña la tipificación de algunos delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos, y entre estas figuras, la del "acceso ilícito" (Tít. II, Cap. I del Convenio).

La ley 26388 conocida como "ley de delitos informáticos" al modificar el Código Penal argentino permitió adaptar nuestra legislación interna a las demandas del Convenio sobre Cibercriminalidad de Budapest (2001) en materia de fondo.

Ahora bien, la incorporación del artículo 153 bis en el Código Penal argentino generó polémica en la doctrina especializada, es decir, si el puro intrusismo informático o "*hacking*", ¿debe ser considerado delito o no?, y en el supuesto de que la conducta sea sancionada penalmente, ¿qué tipo de pena debe aplicarse al autor del hecho?

Por ejemplo, Eduardo Rosende se expresó en contra de la inclusión de la figura, alegando que aun cuando fuera difícil distinguir el caso en que se constituyera el acto previo de otros más graves, era posible, y resulta inaceptable suplir deficiencias procesales por vía de incriminar autónomamente la mera intrusión que bien pudiera ser un sencillo caso de comprobación de vulnerabilidades de un sistema informático.

Asimismo, una postura interesante sobre la sanción de pena privativa de libertad, establecida por el artículo 153 bis del CP, es la sostenida por los doctores Gutiérrez, Radesca y Riquert, quienes manifiestan que "*si en el delito más leve, básico y de aplicación subsidiaria, se usa la modalidad más grave de sanción, en el resto de las conductas no*

podrá evitarse sin caer en problemas serios de proporcionalidad y, en realidad, se trata de un comportamiento sobre el que se discute si realmente es necesaria la intervención del derecho penal o bastaría con la del contravencional o sancionador administrativo, apareciendo como más lógicas las penas pecuniarias o de inhabilitación que la prisión".

Estos autores también opinan que "*para evitar o corregir posibles extensiones inadmisibles del ámbito de lo prohibido en esta figura de cuestionada inclusión penal, que el análisis del bien jurídico no haga foco, exclusivamente, en el acceso mismo, en la información en si o en la utilidad de los sistemas informáticos y la necesidad de preservarlos. Aunque ello sea merecedor de tutela, luce evidente que esta puede brindarse más eficazmente en el ámbito administrativo, e incluso, contravencional. Preferimos centrar la atención en que la protección penal se haga sin descuidar el contenido mismo que soporta el dato o sistema informático y que, por algún motivo, su titular no lo hace de público conocimiento, restringiendo su acceso en vistas de resguardar su valor confidencial y, con ello, su derecho subjetivo. De esta forma, no nos alejamos de la protección a la intimidad en la sistemática del código, con consideraciones vinculadas al objeto material o a los medios que ... nos acerca a la punibilidad de meras infracciones*".[15]

Si bien considero acertada la represión autónoma del intrusismo informático, comparto la postura de los autores señalados precedentemente, en el sentido de que la pena de prisión resulta desproporcionada para este tipo penal teniendo en cuenta la levedad del mismo. La pena de multa o alguna inhabilitación especial resultarían más razonables para sancionar este tipo de ilícitos, siempre y cuando no se difundan o releven datos protegidos o no se produzcan daños en el sistema accedido.

En síntesis, el acceso ilegítimo a un sistema o dato informático restringido se consuma cuando se entra o accede indebidamente o sin autorización, ya sea violando las barreras de protección establecidas, sea por no estar autorizado a acceder o cuando se excede la autorización que el sujeto activo del ilícito posee (por ej., el usuario autorizado a ver ciertos datos, pero que usando el acceso legítimo lo transforma en ilegítimo). También se configura cuando se accede, simulando ser el usuario legítimo al utilizar el usuario y la contraseña del titular del sistema informático.

Igualmente, conviene destacar que la figura del artículo 153 bis del Código Penal tiene un carácter residual, remanente o subsidiario, ya que la misma excluye la comisión de un daño o relevación de datos protegidos para la configuración del delito. No resulta necesario que se produzca una modificación o alteración del sistema o dato para que exista delito, sino que la mera intrusión informática sin autorización configura una conducta típica en el derecho argentino.

Por último, entiendo que la tipificación del intrusismo informático resulta fundamental para esclarecer ataques como el que sufrió en el año 1999 la Universidad Nacional de Río Cuarto (causa "Universidad Nacional de Río Cuarto s/denuncia"). El director del Centro de Cómputos de la casa de estudios denunció que en varias oportunidades había detectado ataques al servidor de la institución, que no se hallaba disponible al público, sino que tenía un acceso administrado a través de claves personales. Si bien se logró identificar al autor del acceso no autorizado, el mismo no fue procesado, porque se resolvió que los hechos investigados no encuadraban en ninguno de los delitos previstos por el Código Penal, debiendo desestimar la denuncia y ordenar su archivo.

(15) Gutiérrez, Ricardo; Radesca, Laura C. y Riquert, Marcelo A.: "Código Penal Comentado" - Revista Pensamiento Penal - consultado el 19/5/2018].

IDENTIFICACIÓN POR RADIOFRECUENCIA, CIBERCRIMEN Y PROTECCIÓN DE DATOS

Analía Aspis(*)

I - INTRODUCCIÓN

Todos los días, las vidas de los consumidores y ciudadanos se encuentran expuestas a un nivel de conocimiento cada vez mayor, a través de la ayuda y la convergencia de las tecnologías digitales en concordancia con un interés creciente de los vendedores corporativos en obtener información cada vez más precisa sobre ellos. Es innegable que las tecnologías de la información y comunicación (TIC) ofrecen al sector empresarial un poderoso medio para conocer muchos aspectos de la vida y hábitos de los consumidores. En este contexto, la tecnología de identificación por radiofrecuencia (RFID, por sus siglas en inglés) facilita una variedad de propósitos comerciales: desde la identificación y gestión de productos para controlar la cadena de suministro hasta la protección de la autenticidad de la marca de un producto. En comparación con el sistema de código de barras, la RFID otorga beneficios a largo plazo en la gestión empresarial, como aumento en eficiencia y transacciones personalizadas con potenciales clientes y consumidores. En 2006, IBM recibió la aprobación de una patente denominada "identificación y seguimiento de personas usando artículos etiquetados con RFID". El objetivo que constaba en tal documento hacía referencia a la "*recolección de información y supervisión del movimiento de los consumidores en el marco de una tienda comercial u otras áreas públicas y privadas*".

(*) Abogada. MBA en Derecho, Criminalidad y Seguridad en Nuevas Tecnologías (UNIL). PhD Candidate (Universidad de Estocolmo y UBA-CONICET). Investigadora (UBA). Presidenta y fundadora de la Fundación Weiba para el desarrollo social a través de la tecnología

RFID es la sigla de *Radio Frecuency Identification*, que en castellano suele denominarse como "Identificación por Radiofrecuencia". Esta tecnología se basa en la utilización de un pequeño chip que es adherido a un producto, lo que permite su rastreo y localización. Aunque dicha tecnología sugiere orígenes posmodernos, la realidad denota que la misma no es tan novedosa: desde la década del cuarenta los militares estadounidenses utilizaron este sistema durante la Segunda Guerra Mundial para el reconocimiento a distancia de sus aviones.(1)

Sin embargo, en la actualidad esta tecnología ha ganado el interés de la industria(2), que confía en ella como un medio para optimizar la trazabilidad de todas las mercancías en toda la cadena de distribución, debido a que los progresos de la miniaturización(3) y la reducción de los costos de la fabricación de los chips abren hoy grandes posibilidades, desde su utilización en el proceso de reciclado -para facilitar la tarea de selección y separación de materiales- hasta el control de la temperatura de los alimentos e incluso como medio de pago. Según lo declarado por el grupo de trabajo del artículo 29 de la Unión Europea (UE), "*las funciones específicas que las etiquetas RFID pueden otorgar en los distintos sectores de la industria y comercio, no solo están aumentando las posibilidades de su desarrollo sino que todavía tienen tiempo y espacio para emerger*"(4). Los analistas han identificado lo que consideran las tres fases distintivas de inserción de la RFID en las economías nacionales de los países en desarrollo: la prueba piloto inicial y experimentación de RFID (2003-2005), seguida por una fase de suministro de infraestructura de la cadena (2007-2012), para finalmente la implantación de un marcado generalizado a nivel de artículo (2003-2017). Por último, el informe de la UE señala que la tecnología RFID contribuirá a la realización de la computación ubicua (*ubiquitous computing*), lo que significa que los nuevos tipos de equipos estarán dotados de un etiquetado casi invisible pero omnipresente en la vida cotidiana de las personas, que obtendrán el beneficio de los servicios brindados por estos. De esta manera, las tecnologías relacionales se presentan así como la llave para potenciar las relaciones comerciales con los consumidores, convirtiéndolas en más íntimas y fidelizadas. También se destaca su consideración por parte de los gobiernos para la implementación de las mismas como instrumentos colaborativos para sus políticas públicas, como pasaportes, licencias de conducir y documentos de identidad.

El propósito de la ponencia es presentar una primera aproximación a la temática RFID y su relación con posibles ataques informáticos relacionados con el cibercrimen, en un ambiente RFID como referencia de todos aquellos ambientes inteligentes que puedan

(1) En 1969, Mario Cardillo registra en EE.UU. la primera patente con tecnología RFID

(2) Las corporaciones están invirtiendo en la tecnología RFID: las cifras proporcionadas por los analistas de mercado predicen un aumento enorme de este durante la próxima década. De acuerdo con Gartner Studio (2005), los ingresos del mercado de RFID crecieron más del 33% entre 2004 y 2005 (que representan USD 504 millones en 2005) y tendrá un valor de USD 3 millones para 2010. Por su parte, la consultora IDTechEx predice un mercado global de RFID de USD 26,23 mil millones en 2016 y un número total de etiquetas de salida de 585 miles de millones

(3) Dependiendo del tamaño, tipo y antena del chip, el mismo es susceptible de rastrearse desde una distancia de entre 2 cm hasta los 13 m e incluso varios km en sistemas más complejos. Su estructura es pequeña y, tal como se está avanzando en esta materia, en poco tiempo podrían ser considerados virtualmente invisibles

(4) Dict. 5/20 relativo a la Propuesta de la Industria para un Marco de Evaluación del Impacto sobre la Protección de Datos y la Intimidad en las Aplicaciones Basadas en la Identificación por Radiofrecuencia. Informe del grupo de trabajo - pág. 5 - ver en: ec.europa.eu - Consultado el 26/9/2013

estar relacionados con la actividad de los consumidores. Se pretende iniciar un nuevo debate sobre la privacidad en un nuevo marco de análisis del siglo XXI por medio de la concepción integradora de Internet, así también como la criminalización del tratamiento no autorizado de datos personales. Para ello se presentará en primer lugar una introducción y explicación sobre el funcionamiento de la RFID como así también ejemplos sobre sus aplicaciones más usuales. En segundo lugar se establecerá una relación entre la capacidad tecnológica de los chips y su vinculación con posibles ataques informáticos. En tercer lugar, se presentarán las principales soluciones -tanto jurídicas como de gestión- que existen en la actualidad como marco de aplicación preventiva o condenatoria de actos delictivos relacionados con el sistema RFID. Cabe destacar que, al contar la presente tecnología con más amplio desarrollo en Estados Unidos y países de Europa, se han seleccionado por cuestiones metodológicas ejemplos de referencia en relación con tales contextos, lo cual no implica que el mismo análisis pueda realizarse en otros países que cuenten ya con ejemplos prácticos de la aplicación de la RFID. Por último, se presentarán conclusiones y propuestas para futuras líneas de investigación.

II - INTRODUCCIÓN A LA TECNOLOGÍA DE IDENTIFICACIÓN POR RADIOFRECUENCIA

La tecnología RFID utiliza ondas de radio para identificar de manera inalámbrica, sin ningún tipo de contacto, sin visibilidad y en forma automática objetos o personas vinculadas con un *tag*[5] (en adelante tag) RFID, ya sea por estar incorporado al producto, a su empaquetado, o algún producto que una persona lleve consigo o incluso a la persona misma[6]. Para llevar a cabo su objetivo de identificación única de objetos utiliza una porción del espectro electromagnético. Consiste en dos partes: un tag que contiene un número de identificación y un lector -que funciona como un escáner- que emite una secuencia de radio para captar el número de identificación emitido por el *tag*. Este número será ulteriormente utilizado para el procesamiento de información en una o más bases de datos. El sistema se encuentra diseñado para que ningún tipo de intervención humana sea llevada a cabo.

Un típico *tag* RFID consiste en un circuito pequeño que contiene una antena de radio, con la capacidad de transmitir un único número de serie desde una distancia determinada hacia un dispositivo de lectura, que emite la petición de envío de datos. El *tag* o microchip tiene un tamaño aproximado de 1/3 de mm, y puede ser fácilmente introducido en productos o en sus correspondientes empaquetados y en todos aquellos objetos que las personas puedan llevar consigo, hasta incluso debajo de la piel. Existen tres tipos de *tags* RFID, que se diferencian en la forma mediante la cual se comunican o inician la comunicación con el lector. Los *tags pasivos* no poseen fuente de energía propia (no tienen batería) y, en consecuencia, no inician comunicación alguna, siendo utilizados generalmente para diferentes aplicaciones, como el acceso a edificios, ingreso a lugares

(5) El vocablo *tag* hace referencia a un microchip. La empresa EPC Global Inc. es la responsable del desarrollo de los estándares de los *tags* RFID. La empresa surge como resultado de una joint venture entre UCC y EAN, ambos organismos que regulan el uso del código de barras en los EE.UU. y el resto del mundo. La tendencia actual indica un ascenso en el remplazo de los códigos de barras por *tags* RFID. Para mayor información consultar: epcglobalinc.org - Consultado el 9/7/2013

(6) Es el caso de los microchips subcutáneos, que voluntariamente una persona decida insertar en su organismo o en forma obligatoria, como en determinadas cárceles de EE.UU.

con tickets y seguimiento de productos en la cadena de consumo. Los *tags semi-pasivos*, tanto como los pasivos, no inician la comunicación con el lector por sí mismos pero en su caso sí poseen baterías. Estos *tags* pueden ser combinados, por ejemplo, con sensores[7], con el fin de crear un *smart dust* -pequeños sensores inalámbricos que pueden monitorear estados ambientales-. Por último, los *tags activos* sí inician por sí mismos la comunicación con el lector y generalmente poseen una fuente propia de energía. Tienen la capacidad para comunicarse a larga distancia -100 o más pies[8]-. Si bien se ha comparado la RFID con los códigos de barras, existen diferencias entre ellos. En primer lugar, con la RFID cada producto tiene un número de identificación único, mientras que con el actual código de barras cada producto tiene el mismo número identificativo que cualquier otro del mismo lote de producción. En segundo lugar, un chip RFID puede ser leído a cierta distancia[9], lo cual no es posible con el actual diseño de código de barras. Por último, un *tag* puede estar dotado de hasta 512 bits de memoria y una antena sensible a las ondas de radio, por lo que las etiquetas electrónicas permiten comunicar a distancia los datos que contienen, sin necesidad de una batería o corriente continua, ni siquiera un lector óptico.

Para obtener la información alojada en el *tag* resulta necesario un lector. Un típico lector es un instrumento que tiene una o más antenas con capacidad para emitir ondas de radio y recibir señales desde uno o más *tags*, lo cual permite la recolección de datos en una o más redes determinadas. Dichos datos, una vez recolectados, son alojados en una base de datos donde, según las circunstancias y el consentimiento brindado, pueden llegar a ser objeto de tratamiento y procesamiento ulterior.

III - APLICACIONES RFID

A medida que la RFID es vista como una tecnología revolucionaria respecto de otras existentes en el mercado, un grupo de organizaciones, compañías y empresas ha comenzado a hacer uso de la tecnología por medio de diferentes aplicaciones. Si bien las pioneras han sido las empresas de transporte de mercaderías, en la actualidad existe toda una gama en materia de aplicaciones informáticas. Los siguientes ejemplos intentan ilustrar alguno de los escenarios en los cuales en la actualidad ya es posible experimentar las ventajas de la RFID. Para su mayor comprensión se encuentran divididas según las principales categorías, dependiendo de la utilización de la tecnología en una situación dada.

(7) Por ejemplo, en el caso de SHARP, los *tags* RFID se utilizan para recolectar información sobre la interacción de determinados objetos con un ambiente determinado, y a su vez se utilizan sensores para la recolección de otros datos, como por ejemplo la temperatura o intensidad de la luz

(8) Un ejemplo de tales chips son los utilizados para el pago automático en las carreteras, como los Northeast's E-ZPass, los cuales se encuentran en los autos para que los conductores no se vean obligados a frenar para pagar el impuesto de peaje en la ruta

(9) Así, por ejemplo, se acabarían las colas en las cajas del supermercado porque el contenido de los carros se identificará a distancia con una sencilla lectura por radio. Investigaciones en Alemania ya se encuentran realizando experiencias piloto sobre supermercados inteligentes que facilitan notablemente el ahorro de tiempo en línea de caja y gestión personal del proceso de compra por parte del consumidor

a) Transporte

Transporte público

En Europa, muchas organizaciones de transporte público (bus, ferry, metro) han reemplazado el *ticket* de papel tradicional por tarjetas plásticas tagueadas: el dinero debe ser depositado previamente en dicha tarjeta, ya sea con pago en efectivo, tarjeta de débito o crédito. Incluso algunas tarjetas cumplen la función de tarjeta de compra para otros productos fuera del transporte público. Para citar algunos ejemplos, podemos mencionar en Europa el caso de *VRR/ VRS Card* en North-Rhine-Westphalia[10] (Alemania), SL (Suecia), *SI Pass* (Italia) and OV-chipkaart (Países Bajos). Otro ejemplo es el Lufthansa *Ticketless flying*. La tarjeta tagueada combina la función de ticket, credencial de pasajero frecuente y tarjeta de crédito para la obtención de beneficios. El sistema le permite al cliente realizar el *check in* a último minuto y en solo 10 segundos puede gozar de los beneficios con tan solo presentar su tarjeta en la *Chip-in-Terminal*.

"Electronic toll collection"

Esta aplicación tiene como objetivo eliminar los retrasos en las carreteras que se generan cuando se debe realizar algún pago en las oficinas de peaje. Los lectores, situados en posiciones estratégicas, reconocen el *tag* inserto en el auto del conductor, y una vez que realiza la lectura correspondiente, se produce el débito del dinero del impuesto, sin necesidad de que el auto deba frenar en ningún momento. También se encuentra previsto para reconocimiento de autos al momento del ingreso a edificios y oficinas.[11]

Permisos de "parking"

Cabe mencionar la opción de habilitación de espacios de aparcamiento por medio del reconocimiento de un chip determinado. El *Parking and Transportation Services* de la Universidad de Arizona ha comenzado a utilizar la tecnología RFID; en lugar del *parking* tradicional, un pequeño chip se adjunta al vehículo, y el conductor solo tiene que estacionar el automóvil y automáticamente la puerta de entrada se encuentra habilitada para entrar a las dependencias.[12]

(10) Las empresas alemanas Verkehrsverbund Rhein-Ruhr (VRR) y Verkehrsverbund Rhein-Sieg (VRS) son el mayor ejemplo de adopción de *tags* RFID a gran escala, tanto en trenes como buses, con un alcance de resultados que incide en 10.6 millones de habitaciones y 1.1 billones de pasajeros por año

(11) En la actualidad la más conocida aplicación RFID para el pago en las estaciones de servicios o gasolineras es el Speedpass. Si bien el sistema todavía no ha sido desarrollado en Europa, más de 6 millones de lectores Speedpass han sido vendidos en los EE.UU., abarcando 8800 locales Exxon y Mobil. Otros 2 millones de Speedpass han sido vendidos en Canadá, Singapur y Japón para ser utilizados en más de 1.600 locales en dichos países. El E-ZPass (EE.UU.), e-TAG (Australia), Liber-T (Francia), SI Pass (Italia) son otros ejemplos de aplicaciones similares de la RFID en materia de transporte

(12) Ver en: parking.arizona.edu - Consultado el 5/7/2013

b) Transacciones financieras

Billetes RFID

Aunque el proyecto no se ha concretado aún, el Banco Central Europeo ha propuesto introducir el chip RFID a fin de evitar falsificaciones de billetes, recuperar dinero robado y facilitar el monitoreo de la emisión monetaria.

Casinos

En ciertos casinos ya se ha implementado la introducción de un *tag* en las fichas de juego para estudiar los movimientos de los jugadores, así como también para evitar jugadas desleales.

Tarjeta de crédito RFID

Las tarjetas de crédito tradicionales pueden contar con un chip RFID incluido y ser utilizadas como medio de pago sin necesidad de utilización de la tradicional banda magnética.

Pagos automáticos

El sistema de pagos automáticos se especializa en crear una forma de pago automática que solo requiere la presentación de una tarjeta tagueada. En Estados Unidos, la *General Services Administration Smart Card Program*[13] provee tarjetas RFID habilitadas para realizar este tipo de transacciones. A su vez, Mastecard ha presentado un producto que permite combinar los servicios de la tarjeta de crédito -por medio de teléfonos celulares- con la RFID, con el fin de facilitar la realización de las compras, directamente presentando el celular y en un solo paso (*Mobile MarterCard PayPass*).[14]

Tickets

Si bien en la sección anterior se hizo referencia al uso de RFID en el transporte público, la aplicación referida a los tickets hace alusión a otros sectores, como el del entretenimiento. El estadio *Madejski Stadium* en el Reino Unido es un ejemplo de su uso: el ticket tagueado no solo permite el acceso al estadio sino que también proporciona un medio de fidelización del visitante (carnet de socio), medio de pago, permiso de entrada y marketing directo[15]. También en el evento de la copa del mundo, el *FIFA World Cup*

(13) Para mayor información sobre el programa ver smart.gov - Consultado el 4/7/2013

(14) En EE.UU. existen ya estados que han adoptado el sistema de pago automático, como Chicago, Nueva York, San Francisco, Seattle y Washington D.C. En 2001 Exxon Mobile comenzó sus pruebas de implementación en 450 McDonalds en Chicago y en 2003 en los supermercados Stop & Stop con el fin de evaluar si el sistema de pago podía extenderse a sectores más complejos. Según lo expresado por Joe Giordano, vicepresidente del plan de desarrollo, los consumidores expresaban que estaban interesados en recibir ofertas y sugerencias acordes con su perfil de compras. Para mayor información sobre Smart Card Alliance visitar smartcardalliance.org - Consultado el 23/9/2013

(15) Para mayor información ver CORDIS Europe, disponible en cordis.europa.eu - Consultado el 23/9/2013

ticketing Centre emitió y puso a la venta en Alemania tickets RFID para evitar falsificaciones de las entradas para los partidos de fútbol.[16]

c) Salud

Si bien las aplicaciones en el ámbito de la salud son muy recientes, las posibilidades que ofrecen resultan no solo prometedoras sino también variadas, desde el monitoreo (*tracking*) de los productos farmacéuticos y materiales de laboratorio a todo el proceso de aplicación –con el fin de reducir errores humanos-[17][18].Como ejemplo, puede citarse el caso del sector de cuidados médicos en el *Jacobi Medical Center* en Nueva York, donde las enfermeras utilizan una Tablet para identificar a cada paciente con el medicamento que les debe ser provisto, el cual se encuentra tagueado con su correspondiente identificación, lo que permite que cada paciente reciba la dosis exacta y que solo la medicación que haya sido prescripta le sea entregada. Al mismo tiempo, se genera un registro de historia clínica digital que la enfermera -o cualquier otro integrante del equipo médico- puede consultar. A su vez, la *Food and Drug Administration* se encuentra evaluando la posibilidad de taguear los medicamentos, puesto que su fin reside en comenzar a generar registros sobre qué medicamentos, por cuánto tiempo y exactamente en qué lugar de las góndolas de las farmacias los mismos se ubican[19]. Otros ejemplos han sido publicados en la revista *eWeek Report*, que señalan que la adopción de etiquetado RFID por parte de determinadas farmacias tiende a reducir robos como así también el contrabando de medicamentos.

d) Comercio

Seguimiento de productos y objetos

Este ha sido uno de los más extensos usos de la RFID, ya que facilita el seguimiento de materiales y productos en todo momento y lugar de la cadena de distribución y consumo, y resultan diferentes los experimentos y puestas en marcha de comercios inteligentes en diferentes países, inclusive en la industria del lujo debido, a sus altos costos y la facilitación de identificación de sus productos (por ejemplo, joyerías)[20][21],

(16) European Parliament, Scientific Technology Options Assessment (STOA): "RFID and Identity Management in Everyday Life: striking the balance between convenience, choice and control" - Junio 2007 - pág.43. Para otros ejemplos de aplicaciones RFID en el sector entretenimiento ver: europarl.europa.eu - Consultado el 7/7/2013

(17) Crounse, Bill: "RFID. Increasing patient safety, reducing healthcare costs" - disponible en microsoft.com - Consultado el 7/7/2013

(18) Un estudio realizado por Gartner, Inc, consultora líder en investigaciones relacionadas con la industria de la tecnología de la información y la comunicación, ha concluido que "*si la implementación de la tecnología RFID continúa creciendo, es casi certero que será una herramienta esencial para la disminución de errores humanos, mejorar la eficiencia de los equipos médicos y reducir costos*". Ver Hieb, Barry R., M.D. "Medication Administration Uses RFID and Bar Codes to Save Time and Money" - Gartner Research Paper Number G00127318 - 6/6/2005

(19) Ver "Combating Counterfeit Drugs, A Report of the Food and Drug Administration", Febrero de 2004, en fda.gov - Consultado el 5/5/2013

(20) Ver European passive RFID Market Sizing 2007-2022, febrero/2007

(21) Ver spacecode-rfid.com

brindando la posibilidad de comprobación de autenticidad, *stock* y seguimiento, entre otros. Otros ejemplos de seguimiento remiten al tagueado de equipaje en los aeropuertos[22] o de la correspondencia postal.[23]

IV - EL VALOR DE LOS DATOS PARA LOS CRIMINALES

Más allá de los beneficios comerciales señalados, en los últimos años ha comenzado a surgir cierta preocupación sobre los posibles riesgos derivados del uso de la RFID[24] y su relación con los perfiles de consumidor y la posibilidad de *tracking* de movimientos dentro y fuera de la tienda sin su conocimiento. Si un *hacker* tuviera la posibilidad de acceder y procesar los datos de un *tag*, podría determinar qué productos consume una persona, cuán frecuentemente y en consecuencia dónde el producto -y por extensión el consumidor- circulan. Mediante el procesamiento de datos se podrían realizar inferencias sobre los ingresos del consumidor, estilo de vida, salud, hábitos de consumo y posicionamiento espacio-temporal y posteriormente vender dichos datos a terceras personas, incluidas las corporaciones. Aún más, el producto puede ser relacionado con información personal, como detalles de tarjeta de crédito, y relacionarla con otras bases de datos existentes. Lo antedicho ha introducido el debate sobre la tecnología RFID y su relación con el marco jurídico aplicable en ocasión de posibles amenazas a la privacidad, dada su característica de poder localizar y observar los movimientos de una persona en tiempo real.

En ese sentido, el valor de los datos, tanto en el ciberespacio como en las redes inalámbricas, se encuentra también relacionado con el cibercrimen, debido a que los delincuentes informáticos parecieran elegir nuevos objetivos para sus ataques en las nuevas plataformas móviles o las redes sociales informatizadas, donde el usuario o consumidor se encuentra menos advertido de los riesgos, e incluso los desconoce por completo. Por su parte, la llegada del protocolo de Internet IPv6 permite la integración de millones de objetos en redes, como así también admite nuevas oportunidades de ataque donde, entre los blancos más atractivos, se encuentran los *smartphones* combinados con *tags* RFID[25]. Asimismo, los datos de los consumidores encuentran en el mercado un valor importante en términos de información. Mientras que las computadoras son esenciales

(22) El aeropuerto McCarran International en Las Vegas fue el primero en facilitar el uso de la tecnología RFID en los equipajes. Ver "Las Vegas Airport Bets on RFID, RFID journal", (6/11/2003), disponible en rfidjournal.com - Consultado el 9/7/2013. Otra empresa que se encuentra en fase de experimentación es Delta AirLines, que se encuentra desarrollando un sistema que permitirá la impresión de *tickets* con un *tag* incluido y la inserción de lectores en sectores estratégicos del aeropuerto y los aviones. Ver "RFID Journal, Delta Takes RFID under its Wings", 20/6/2003, disponible en rfidjournal.com

(23) El US Postal Service en EE.UU. se encuentra considerando la posibilidad de utilizar la RFID para la gestión de su correspondencia. Ver "RFID Streamlines Processes, Saves Tax Dollars", disponible en sun.com

(24) Ver Langheinrich, Marc: "RFID and Privacy, Institute for Pervasive Computing" - ETH - Zurich, disponible en vs.inf.ethz.ch - Consultado el 1/7/2013

(25) Existen dos formas de integrar un sistema RFID en un *smartphone:* con un RFID *tag* o con un lector. Un *smartphone* con un *tag* RFID se conecta a una red GSM u otra red inalámbrica, lo cual permite su identificación singular. A su vez, más allá de la antena propia del teléfono, el mismo posee una antena para comunicarse con el o los lectores que se encuentren en un lugar determinado.

para esta última fase de recopilación de datos, la necesidad de recopilar e intercambiar información financiera no es nueva, así como tampoco lo son los nuevos ataques a los sistemas que almacenan estos datos que, sin embargo, presentan una nueva variante en el caso de ambientes inteligentes.

V - RFID, PROTECCIÓN DE DATOS Y CIBERCRIMINALIDAD

Los sistemas RFID son un objetivo atractivo para los cibercriminales, ya que los datos alojados en el *tag*, pueden ser de carácter financiero o personal -hasta incluso información importante para la seguridad nacional, como por ejemplo, los pasaportes-. Agrava esta situación la posibilidad de que el *malware* RFID podría causar más daño que el malware tradicional basado en computadoras normales: esto es así puesto que el malware utilizado para atacar una RFID tiene también efectos en el mundo *offline*, y en consecuencia, los objetos tagueados son susceptibles de daño. Tal como lo ha señalado la *Organization for Economic Co-operation and Development* (OCDE), los sistemas RFID se encuentran, tal como cualquier otro tipo de sistema de información, sujetos a riesgos de seguridad[26]. En este contexto, la RFID, como una herramienta más para identificar personas u objetos, toma también protagonismo para aquellos que pretendan cometer un delito informático.

Desde el punto de vista del consumidor, si bien no todos los usos de la RFID devienen en implicancias relacionadas con la privacidad, lo cierto es que, al tener dichos sistemas la habilidad de recolectar o procesar información relativa a un individuo identificado o identificable, transforma su status en vulnerable para su vida íntima debido a que la recolección y procesamiento de datos puede realizarse sin su consentimiento[27]. Si un delincuente accediera o tomara control del sistema RFID utilizado por una empresa -y en consecuencia de los datos transmitidos por las etiquetas-, tendría la posibilidad de determinar los productos o compras de los consumidores, con qué frecuencia se utilizan estos productos e incluso cuándo el producto -y por extensión el consumidor- realiza movimientos. Mediante la agregación de datos para formar perfiles de consumidores, las empresas o un tercero podrían manipular los datos para hacer suposiciones deductivas sobre los ingresos de los consumidores, la salud, estilo de vida, hábitos de compra y ubicación. Esas bases de datos, e incluso la etiqueta, pueden ser objetivos de hackeo. Estas preocupaciones son incluso más pertinentes cuando las tecnologías se combinan, integrando y conectando, de forma invisible y remota, la computación ubicua. La comprensión de la cibercriminalidad, con referencia a la necesidad de la protección de la intimidad digital, reconoce que los datos personales son activos intangibles de gran valor,

Cuando el teléfono envía información al lector, la misma, luego de ser recibida, es susceptible de ser procesada y reenviada al teléfono, que la incorpora en su sistema de datos y al mismo tiempo procesa la información obtenida de los lectores. Por su lado, un smartphone con un lector RFID, tiene la capacidad de lectura de otro *tag* RFID según un uso determinado y estar al mismo tiempo conectado inalámbricamente con otros servicios

(26) "Organisation For Economic Co-operation and development, RFID Radio Frequency Identification, OECD Policy Guidance A Focus on Information Security and Privacy Applications, Impacts and Country Initiatives, OECD Ministerial Meeting on the Future of the Internet Economy" - Seoul - 17-18/6/2008 - pág. 4, disponible en oecd.org - Consultado el 10/7/2013

(27) El debate sobre el consentimiento expreso o tácito de un consumidor al ingresar a una tienda comercial merece un tratamiento especial de doctrina que excede el propósito de la presente ponencia

tanto para empresas (como personas jurídicas) como para los delincuentes. Para el propósito del presente trabajo, se citan las amenazas más importantes y que pueden ser susceptibles de ser consideradas como una actividad delictiva por parte de las figuras precedentemente mencionadas.

a) Tratamiento de datos por medio de la ocultación de *tags*

Para propósitos tales como la confección de inventarios clandestinos o la minería de datos, las empresas pueden recopilar información acerca de un determinado producto y, dependiendo de las circunstancias, de la persona que tiene en su poder el producto, sin el conocimiento de esta. Como las ondas de radio viajan fácilmente y de manera silenciosa a través de diferentes materiales (telas, plásticos, cartones, etc.) es posible interceptar la comunicación entre el lector y la etiqueta RFID añadida a la ropa o fijada a los objetos contenidos en monederos, bolsas de la compra, maletas, etc. Por otra parte, también puede acontecer que, una vez que la información recopilada sea alojada en una base de datos, la misma sea susceptible de un ataque informático.

b) *Tracking* y monitoreo

Una aplicación RFID puede recolectar grandes cantidades de datos. Si un artículo etiquetado es, por ejemplo, comprado en la línea de caja con tarjeta de crédito o en combinación con el uso de una tarjeta de fidelidad o de débito, es posible vincular el identificador único de ese elemento con la identidad del comprador. Los datos personales obtenidos a través de RFID se podrían utilizar para crear un perfil determinado de una persona, por ejemplo, para evaluar el valor de un consumidor para una empresa o para ser vendidos a un tercero[28]. La generación de perfiles puede incluir segmentación de consumidores, estigmatización y focalización individualizada[29]. Asimismo, dicha información puede ser vendida a otras empresas con motivos relacionados con el *marketing*.

c) *Snooping*

Las capacidades de la tecnología RFID permiten acceder a detalles relacionados con los hábitos de un consumidor inimaginables unas décadas atrás. Las tarjetas de fidelización con RFID permiten a las empresas identificar a los clientes, y cambian los precios de los productos según el perfil de compra de los clientes. Los atacantes pueden crear auténticas etiquetas RFID y reescribir los datos de la misma. Una simulación de ataque por suplantación fue realizada recientemente por investigadores de la Universidad Johns Hopkins y RSA Security[30]. Los investigadores clonaron un chip RFID mediante el

(28) Preocupación sobre la generación de perfiles y monitoreo fueron ya advertidos en 2005 en el reporte de la U.S. Government Accountability Office GAO ante el Congreso de los Estados Unidos, el cual señalaba que el uso de *tags* y bases de datos vinculadas genera importantes problemas de seguridad, confidencialidad, integridad de los datos alojados en los *tags* y las bases de datos así también como incertidumbre respecto de la protección de dicha información. El reporte completo se encuentra disponible en gao.gov - Consultado el 25/5/2013

(29) "A Holistic Privacy Framework for RFID Applications D12.3", disponible en fidis.net - Consultado el 11/7/2013

(30) Bono, S.; Green, M.; Stubble_eld, A.; Juels, A.; Rubin, A. y M. Szydlo: "Security analysis of a cryptographically enabled RFID device" en 14th USENIX Security Symposium - Baltimore, Maryland, USA - julio-agosto/2005. USENIX. págs. 1/16

descifrado del identificador que se utiliza para comprar gasolina, así como también llevaron a cabo el desbloqueo del sistema de inmovilización del vehículo -también basado en RFID-.

d) *Cracking*

La Universidad Johns Hopkins y RSA Laboratories en los EE. UU. llegaron a la conclusión de que mediante el uso de un dispositivo electrónico económico -de alrededor de U$S 200- un delincuente podría *crackear* la clave criptográfica de una etiqueta RFID y luego usar la información para fines personales, de consumo o sustitución de identidad. Dado que la tecnología de etiquetas es todavía relativamente joven, todavía nos encontramos en una etapa incipiente, donde no se pueden vaticinar qué nuevas técnicas de *cracking* podrían surgir.(31)

e) *Cloning*

Ya en febrero de 2007, en la Conferencia RSA, Chris Paget, Director de Investigación y Desarrollo de IOS, demostró cómo un dispositivo portátil del tamaño de un teléfono celular, que cuesta alrededor de veinte dólares, pudo leer la información personal codificada en los chips RFID utilizados por HID Global ProxCards.(32)

f) *Sniffing*

Las etiquetas RFID están diseñadas para ser leídas por cualquier dispositivo de lectura compatible, sin el conocimiento del portador. Una controversia reciente se ha desatado en relación con los pasaportes digitales y demás documentos de identidad personal.

g) *Malware*

Los investigadores de la Universidad Libre de Ámsterdam han demostrado que un virus instalado en una etiqueta RFID puede infectar a una base de datos (*back-end*) a través del lector de RFID, en función de ciertas vulnerabilidades en el *software* del *tag*.

h) Denegación de servicio

Un envío masivo de información puede ocasionar el bloqueo de una etiqueta RFID e interrumpir la comunicación con el lector y/o la base de datos. En estos casos, el lector no podrá recibir la información enviada por las etiquetas, lo que hace que el sistema no esté disponible para autorizar usos.

(31) Según Garfinkel, Simson and Holtzman, autores del libro RFID. Aplicaciones, seguridad y privacidad, la tecnología RFID importará cambios e innovaciones en el proceso de compra y circulación de las personas. Garfinkel, Simson and Holtzman, H. (2005): "Understanding RFID Technology", en Garfinkel Simson; Rosenberg, Beth (Coords.): "RFID Applications, Security, and Privacy" - Ed. Addison-Wesley Professional - Boston - pág. 262

(32) Ver Roberts, Paul F.: "Black Hat Dispute Stirs RFID Security Awareness" - Infoworld - 28/2/2007, www.infoworld.com - Consultado el 15/5/2013; ver también Krebs, Brian: "RFID Flap Silences Security Researchers, Security Fix" - 27/2/2007, disponible en blog.washingtonpost.com/securityfix; Lemos, Robert: "Legal Threats Scuttle RFID Flaw Demo" - Security Focus - 27/2/2007, disponible en securityfocus.com

VI - PERSPECTIVAS LEGALES PARA COMBATIR EL CIBERCRIMEN VINCULADO CON TECNOLOGÍA RFID

Como afirma el profesor Wall[33], las transformaciones particulares que afectan a la arquitectura digital y la oportunidad delictiva son el crecimiento de la convergencia de tecnologías, la importancia de la transferencia de información y la intermediación de la adquisición de información, así también como la vigilancia de datos a través de la minería de datos y la globalización. En este sentido, surge una pregunta: ¿cuáles son las políticas actuales que existen en el entorno RFID para hacer frente a las posibles amenazas a la privacidad y a los ataques cibernéticos a los que los consumidores pueden estar expuestos?

En primer lugar, hay que destacar que los diversos delitos relacionados con la tecnología RFID pueden ser abordados desde diferentes perspectivas según el marco jurídico aplicable, a saber: la legislación relativa a los datos personales, la legislación específica en materia penal, la autorregulación de la industria o bien por medio de soluciones tecnológicas, que pueden proteger todo o conjuntamente con las leyes que atacan a la RFID. En este sentido, las políticas de protección RFID no deben verse únicamente desde la perspectiva de la lucha contra la cibercriminalidad, sino también desde aquella vinculada a la protección de los derechos fundamentales y de las libertades civiles, que incluyen la libertad de circulación, el derecho al conocimiento y a la información y el derecho al respeto de la vida privada, familiar y de la correspondencia. Sin embargo, lo cierto es que se presenta en este nuevo contexto la necesidad de poder garantizar la protección de los datos personales y la intimidad de los ataques externos que pueden implicar un detrimento a la libre determinación, a la democracia, a la libertad y, en consecuencia, a la dignidad humana. Puesto que hasta el momento tanto en la UE y los Estados Unidos ha habido una falta de consenso con respecto al mejor procedimiento para dicha protección, se presentarán a continuación las principales tendencias en materia regulatoria.

a) Legislación relacionada con la privacidad

Hoy en día, la mayor preocupación por parte de la doctrina en materia de privacidad y el uso de la RFID ha sido el estudio de los diferentes marcos legales de aplicación de reglas nacionales sobre protección de datos. Si bien el sistema europeo y el estadounidense cuentan con diferencias conceptuales en relación con el abordaje de la temática, lo cierto es que ninguno de los dos cuenta hasta la fecha con una legislación específica en materia de RFID. Cabe resaltar la excepción de ciertos estados de Estados Unidos donde, si bien se han regulado ciertos aspectos específicos del uso de los *tags*, aun así se pierde efectividad cuando el caso particular se ve confrontado con leyes de mayor jerarquía.

b) Leyes relacionadas con la criminalidad

Sorprendentemente, los aspectos penales de la RFID también han sido poco estudiados en la literatura académica o en informes de las asociaciones civiles, donde el debate principal hasta el momento se ha concentrado en cuestiones relativas a la

(33) Wall, David S.: "Cybercrime, Crime and Society Series" – Ed. Polity Press - Cambridge - 2007 - pág. 34

privacidad en internet. Sin embargo podríamos pensar en determinadas situaciones en las cuales pudiera aplicarse la ley penal en ocasión de manipulación de una etiqueta RFID con fines delictivos. Según lo declarado por *Future of Identity in the Information Society*(34), la cuestión más importante reside en evaluar si un *tag* RFID califica como un sistema informático o de información ya que, dependiendo del tipo de etiqueta RFID, algunos de ellos tienen capacidad de procesamiento y por lo tanto podrían ser considerados como sistema informático según la Decisión marco(35) relativa a los ataques contra los sistemas de información (en adelante, la Decisión marco). La norma establece en su artículo 1(a) que será considerado como sistema de información a "*todo aparato o grupo de aparatos interconectados o relacionados entre sí, uno o varios de los cuales realizan, mediante un programa, el tratamiento automático de datos informáticos, así como los datos informáticos almacenados, tratados, recuperados o transmitidos por estos últimos para su funcionamiento, utilización, protección y mantenimiento*". En el mismo sentido sería de aplicación el artículo 1(a) del Convenio sobre la Ciberdelincuencia de 2001 ya que la mayoría de las etiquetas RFID cumplen con la definición, en tanto son parte de un sistema de etiquetas y lectores RFID que utilizan un *software* para procesar los datos de la etiqueta(36). En consecuencia, la manipulación de una etiqueta RFID califica tanto como una injerencia ilegal en el sistema como una intromisión ilegal. A su vez, en aquellos casos donde manipular las etiquetas RFID más triviales no sería considerado como una interferencia del sistema, sí podrían ser considerados como una intromisión no consentida en los datos del titular y, en aquellos casos donde la manipulación de una etiqueta RFID no pudiera ser considerada por sí misma una de tipo penal (por ejemplo, porque la etiqueta no puede considerarse como un sistema de información), aun podría ser ilegal si la interacción con la misma generase ciertas consecuencias. Esto podría suceder en circunstancias de cambio de precio de un producto para cometer un fraude. Del mismo modo, el cambio de una etiqueta de identificación que tiene una función de registro oficial podría calificar como falsificación.

Como se mencionó anteriormente, un criminal puede también realizar labores espías o interceptar etiquetas RFID. Estas actividades reflejan, después de todo, el centro de las preocupaciones de privacidad expresadas por el público y la sociedad civil y su máximo exponente se advierte en los casos de pasaportes tagueados con tecnología RFID. Tal intercepción podría considerarse interceptación ilegal en la mayoría de los sistemas jurídicos, criminalizadas por el artículo 3 de la Convención de la Cibercriminalidad(37), ya sea por intercepción del lector, el *tag* o la comunicación entre ambos.

(34) Rannenberg, Kai; Royer, Denis; Deuker, André (Coords.): "The future of identity in the information society. Challenges and opportunities" - Ed. Springer - 2009 - pág. 54

(35) 2010/0273 (COD) Proposal for a Directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA

(36) Incluso no sería necesario que el *tag* RFID contenga en sí mismo un *software* si cumpliera con el requisito de ser parte de un grupo de objetos interconectados

(37) **Art. 3** - "***Interceptación ilícita***. *Cada parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la interceptación deliberada e ilegítima por medios técnicos de datos informáticos en transmisiones no públicas dirigidas a un sistema informático, originadas en un sistema informático o efectuadas dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos. Las Partes podrán exigir que el delito se cometa con intención delictiva o en relación con un sistema informático conectado a otro sistema informático*"

Lo mismo vale para el acceso a los datos de una etiqueta RFID por medio del uso de un lector no autorizado, donde en estos casos los datos no se interceptan sino que se produce un acceso de carácter ilegal a los mismos. Tanto la Decisión Marco (art. 5), -al menos para los casos que no son de mayor importancia-, como el Convenio de Ciberdelincuencia (art. 2) criminalizarían tales actividades. Cabe señalar que ambos instrumentos destacan que los Estados pueden restringir la prohibición de acceso ilegal en los casos en que se ha infringido una medida de seguridad. Esto implica que las etiquetas RFID sin protección podrían, desde el punto de vista del derecho penal, ser leídas por cualquier persona, incluso sin razón, y solo las etiquetas RFID con alguna medida de seguridad estarían protegidas por la ley penal contra el acceso ilegal.

Por último, no está claro si el bloqueo de la comunicación entre etiquetas y lectores RFID (por ejemplo, mediante la alteración del campo electromagnético) puede tener consecuencias penales. Habría que estudiar caso por caso si este acto puede calificar como una injerencia ilegal en el sistema en los términos de la Decisión Marco (art. 3) y el Convenio sobre Ciberdelincuencia (art.5) -el acto intencionado de obstaculizar o interrumpir el funcionamiento de un sistema de información-. Por ejemplo, cuando se usara un bloqueador para evitar todas las ventas en una tienda de artículos de lujo por varias horas o si activistas de derechos animales bloquearan sistemáticamente la lectura de las etiquetas de ganado en un mercado.

c) Autorregulación de la industria tecnológica

Para los Estados Unidos, y en menor medida en el contexto europeo o latinoamericano, una de las opciones para la aplicación de las normas de protección de la RFID es la autorregulación de la industria tecnológica. Sin embargo, la eficacia de dicha política regulatoria para hacer frente a los problemas de privacidad depende de algunas condiciones que debieran efectivizarse. Por un lado, las empresas deberían voluntariamente adoptar y poner en práctica un conjunto de políticas de privacidad y procedimientos de cumplimiento y mecanismos de aplicación. Por otro lado, los consumidores tendrían que tener la seguridad de que las organizaciones están implementando tales reglas. Asimismo, debiera establecerse el carácter de su cumplimiento, sea voluntario u obligatorio. De esta manera, la autorregulación se presenta como una solución adecuada para complementar medidas reglamentarias preexistentes, en particular en las áreas que son demasiado específicas para ser objeto de una legislación para la implementación de la tecnología RFID en el sector minorista.(38)

Por el contrario, los opositores a la autorregulación alegan que este tipo de medidas pueden no ser suficientes como medio efectivo para la plena aplicación del marco existente para la protección de datos y privacidad, destacando que, incluso si la autorregulación cumpliese con los requisitos mencionados anteriormente, su aplicación sería de todas formas voluntaria y su incumplimiento no puede ser siempre sancionado efectivamente. Además, indica que de todas formas sería todavía necesario adoptar medidas legislativas vinculantes(39), con el fin de garantizar la protección de los derechos individuales a la privacidad y protección de datos.

(38) Un ejemplo de lo señalado se puede advertir en el caso de las líneas directrices de las políticas de actuación publicadas por EPCglobal, las cuales adoptan los principios generales de privacidad -notificación, seguridad, consentimiento- destacados por la OECD

(39) Esto es tanto más necesario en caso de que falle el enfoque de auto-regulado

d) Protección por diseño

Es evidente que las soluciones tecnológicas son importantes para garantizar la privacidad de los consumidores. El debate sobre la intimidad y los ataques criminales ha dado lugar a una gran variedad de propuestas técnicas para proteger los datos RFID que abarcan, además de las medidas generales de seguridad, una serie de tecnologías de privacidad específicas (PET, por sus siglas en inglés) aplicadas a la RFID. Estas impiden la lectura incontrolada de los *tags*, así como permiten evitar los diferentes tipos de ataques a los cuales el sistema pueda resultar expuesto.

Las principales opciones técnicas son las siguientes:

- *Desactivación de etiquetas y comando Kill*. La protección más eficaz de la privacidad para los artículos etiquetados con RFID es la desactivación de la etiqueta, ya que evita de manera fiable la exploración clandestina de los datos de identificación de la etiqueta. Sin embargo, la desactivación es difícil de implementar en la práctica por su coste.(40)
- *La protección física de las etiquetas*. Las etiquetas pueden protegerse con una lámina de aluminio, con el fin de protegerlas de una lectura no autorizada. Sin embargo, esta tecnología no es adecuada para la ropa y otra gran cantidad de objetos, donde el *tag* debe estar activo de manera permanente para el cumplimiento de sus fines en el entorno donde se haya decidido implementarlo.
- *Encriptado*. El cifrado de los datos que se transmiten es un método para proteger un *tag* contra cualquier persona que intente interceptar la comunicación a través del aire (por ejemplo, por medio de un lector no autorizado), aunque no todos los soportes de etiquetas tienen procedimientos criptográficos eficientes.
- *La solución user-model*. Esta solución implica que los usuarios ejerzan un control total sobre las etiquetas RFID a través de mecanismos de autenticación adecuados.(41)

Si bien todas estas soluciones técnicas proponen una alternativa ante el avance del cibercrimen, el profesor Marc Langheinrich, del Instituto Pervasive Computing, en Zurich, indica que el exceso de seguridad puede interponerse en el camino de la usabilidad, confundiendo e incluso desmotivando a los consumidores: "S*i hacemos los artículos etiquetados demasiado difíciles de proteger, las personas no se molestan en hacerlo. Más tecnología significa una mayor complejidad, lo que significa más dificultad, lo que significa menos uso. Necesitamos de esfuerzo cero, soluciones de gestión de cero, y sin dispositivos*"(42), concluye.

VII - CONCLUSIONES

Lo que hay que proteger está en el centro del debate actual sobre la tecnología RFID. La economía digital brinda condiciones óptimas para las actividades con fines comerciales, así también como la inserción de políticas informáticas para fines públicos. Sin embargo,

(40) Para una crítica sobre la opción killing *tag* ver Privacy Rights, RFID Position Statement of Consumer Privacy and Civil Liberties Organizations, abril 17, 08. Disponible en privacyrights.org - Consultado por última vez 9/7/2013

(41) Spikermann, Sarat, Perceived Control: Scales for Privacy in Ubiquitous Computing, disponible en: papers.ssrn.com, última visita 7/7/2013

(42) TACD, RFID and Ubiquitous Computing: How to ensure that RFID also serves consumer interests - Meeting Report - 13/3/2007, disponible en tacd.org, última visita 12/7/2013

estas deben ser complementadas por acciones tendientes a la mitigación de los riesgos de la delincuencia cibernética que pueden sufrir los consumidores, empresas y gobiernos. El potencial de disminución de las actividades delictivas cibernéticas, especialmente aquellas cuya motivación sea financiera, encontrará soluciones por medio de una asociación eficaz en la búsqueda de soluciones por parte del sector público y privado, junto con una colaboración conjunta de todos los interesados. En la sesión de clausura del Diálogo Transatlántico de Consumidores (TACD, por sus siglas en inglés) se señaló la importancia del debate sobre la regulación de la RFID y, por extensión, de las incipientes líneas de investigación sobre nuevas alternativas para la próxima generación de la computación ubicua, donde la RFID jugaría un papel importante por sus numerosos beneficios económicos y sociales que deben ser, al mismo tiempo, protegidos de los ataques de cibercrimen. La prevención por parte de los organismos no gubernamentales, en conjunto con instancias de diálogo con los sectores públicos, se presentan como necesarios para generar conciencia en los consumidores al momento de interactuar con la tecnología. Considero que una labor interdisciplinaria, no solo entre diferentes profesiones abocadas al estudio de la informática sino también entre las distintas ramas del derecho -puede pensarse en un nuevo derecho del consumidor informático o el derecho a la privacidad del consumidor- resulta indispensable para el replanteamiento de la teoría jurídica aplicable a los nuevos escenarios tecnológicos, así como también un minucioso seguimiento y futuras investigaciones relacionadas con los nuevos desafíos que trae internet.

Investigación forense sobre medios digitales

Patricia M. Delbono(*)

I - INTRODUCCIÓN: LA AMENAZA VIRTUAL

El mundo informático, digital o virtual ha adquirido proporciones considerables en los últimos tiempos. Allí, los delitos históricos han pasado a convertirse en delitos cibernéticos, ya que la mayoría de ellos involucran en su accionar un elemento digital, como una computadora, un celular o incluso las redes sociales.

La era informática incorporada a nuestro quehacer cotidiano ha pasado a digitalizar nuestra vida a tal punto que existen casos de consultas médicas o establecimiento de diagnósticos a través de espacios virtuales. Lo cual es en detrimento de una consulta personal con un profesional cualificado que establezca un diagnóstico, no solo por síntomas, sino también con el resultado de estudios complementarios.

Entrando en conceptos delictivos de mayor notoriedad, el *grooming* y el *bullying* han saturado las redes sociales, así como también los abusos, acosos e incluso la muerte. Dichos delitos se originan mediante el intercambio de mensajes en las redes o sitios de comercio electrónico.

(*) Licenciada en Sistemas de Información. Analista en Investigación Criminal. Especialista en Informática Forense. Perito en Sistemas Informáticos (Poder Judicial de la Nación - Distritos San Martín y Morón). Consejera titular (COPITEC)

II - EL ESPECTRO DIGITAL: SU INVESTIGACIÓN

Conforme han ido avanzado los delitos de origen informático, han surgido experticias informáticas para valorar adecuadamente un hecho técnico y determinar cómo pasó, y si es posible encontrar el *humano detrás del teclado* que ha cometido el ilícito.

Bien vale aclarar que los medios digitales no son culpables de hechos técnicos derivados en delitos, sino que son el medio para cometer el ilícito. En algunas oportunidades, los elementos digitales son el fin, en otros, los medios.

Así las cosas, empieza a surgir, tímidamente, la informática forense o cómputo forense, que para dar una definición prolija, Wikipedia ofrece el mejor ejemplo: *"El cómputo forense, también llamado informática forense, computación forense, análisis forense digital o examinación forense digital es la aplicación de técnicas científicas y analíticas especializadas a infraestructura tecnológica que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal. Dichas técnicas incluyen reconstruir el bien informático, examinar datos residuales, autenticar datos y explicar las características técnicas del uso aplicado a los datos y bienes informáticos*".

Una pericia de tipo informática puede desarrollarse sobre cualquier hecho informático y también sobre correos electrónicos, páginas web, redes sociales, programas informáticos y bases de datos, celulares, etc.

III - LAS EVIDENCIAS DIGITALES O EVIDENCIAS IT: QUÉ SON Y QUÉ SE ENCUENTRA EN ELLAS

A modo de resumen, se podría indicar que una evidencia digital es un elemento resguardado en un medio digital. Sin embargo, una apreciación correcta de lo que sería su razón de ser es cualquier información que, ya sea sujeta a intervención de humanos, no se ha extraído de una computadora. La evidencia de IT debe ser en una forma humana legible o capaz de ser interpretada por personas que son expertas en la representación de dicha información con la ayuda de un programa de computadora.

Las características primordiales de toda evidencia digital es que puede ser volátil, anónima, duplicable, alterable, modificable y eliminable. Estos elementos son de vital importancia a la hora de un análisis forense.

1. Fuentes de evidencia digital

Las fuentes de evidencia digital son contenedoras de elementos susceptibles de investigación, por cuanto, en su contenido, se resguarda información que generalmente se asocia al propietario del medio.

En la siguiente tabla se puede observar los medios digitales y cuáles son las fuentes de evidencia que contienen:

Medio digital	Recurso	Evidencia
Computadoras de escritorio y personales	Discos rígidos internos	- Archivos de *logs* - *Cookies* - Archivos ocultos - Historiales de navegación - *Spool* de impresión - Archivos temporales - Archivos de SWAP - Archivos comprimidos - Archivos ocultos - Archivos renombrados - Archivos protegidos con *passwords*
Dispositivo con control de acceso	Pen drive Tarjeta de proximidad Biometría	- Datos identificatorios del usuario - Niveles de acceso - Permisos - Configuraciones
Cámaras digitales	Tarjeta de memoria	- Imágenes - Videos - Sonidos - Fecha y hora de grabación
Tarjetas de memoria		- Imágenes - Documentos o planillas - Fotos
Impresoras - *Scanners*	Tarjetas de memoria en *scanners*	Documentos
Puntos de acceso de *routers wireles*		Archivos de configuración
Diskettes - CD - DVD		
GPS - Celulares	Memoria interna del dispositivo celular Tarjeta de memoria	- SMS - Whatsapp - Telegram - Fotos - Emails - Videos - Notas de voz

Un elemento a destacar de los medios digitales es que en su mayoría contienen números de serie que los identifica, ya sea una computadora, un celular o una memoria. Los CD o DVD también lo poseen y son de importancia capital.

La identificación de un disco rígido, por ejemplo, es importante para la validez de cualquier medio de prueba, ya que una vez retirado de una computadora, ingresa en la cadena de custodia y es esencial para cumplir con los requisitos de identificación al momento de realizar una pericia.

2. Documentando la escena

Un elemento también de importancia, y quizá pocas veces tenido en cuenta, es el documentado de la escena, la elección de los elementos a secuestrar -si fueran objeto de secuestro- y el posterior traslado con su cadena de custodia.

Esta labor, tediosa a veces, tiene un éxito asegurado a la hora de concretar la experticia y que la prueba no se considere nula, por estar viciado su modo de adquisición.

Las tareas a realizar son las siguientes:

- Describir el estado del/de los equipos.
- Fotografiar el/los equipos, escritorio, *mouse*, monitor/celulares, etc.
- Fotografiar frente del equipo, parte trasera, cableados y otros componentes.
- No mover los equipos.
- No correr programas en la PC sospechosa.
- No apagar la PC si está prendida y no prenderla si está apagada.
- No abrir archivos o carpetas del sistema:
  - Cada vez que se explora uno de ellos, cambia la fecha y hora.
- No correr el antivirus:
  - Puede cambiar la fecha y hora de los archivos que escanea.

3. La recolección

Cuando se recolecta la evidencia, y antes de cualquier intervención, el investigador debe asegurarse de no modificar la información contenida en el medio, usando programas especiales para la adquisición.

Por lo tanto, las tres *A* son fundamentales para iniciar la recolección de la evidencia.

- Adquisición: no se debe alterar el archivo origen.
- Autenticación: se debe verificar que el archivo de evidencia adquirido es igual al archivo origen y realizar una copia del archivo de evidencia para trabajar sobre la misma.
- Análisis: se debe inspeccionar el archivo de evidencia sin alterarlo.

4. Resguardar, transportar, almacenar. La cadena de custodia

Identificada la evidencia, los siguientes pasos son: *resguardo, transporte y almacenamiento*. También tienen su peso para el posterior análisis de los elementos secuestrados, ya que garantizan que esos recursos técnicos no sufran golpes o manipulaciones incorrectas y puedan poner en peligro la información contenida en ellos:

- Resguardar:
  - Documentar, inventariar y etiquetar toda la evidencia.
  - Resguardar los medios magnéticos en bolsas antiestáticas.
  - Evitar doblar o arañar *diskettes*, CD, cintas, etc.
- Transportar:
  - Mantener la evidencia electrónica fuera de medios magnéticos.
  - Mantener la evidencia fuera de medios de calor o frío excesivo o en medios de extrema humedad.
  - Evitar durante el transporte, choques o vibraciones excesivas.
  - Mantener la cadena de custodia.
- Almacenar:
  - Establecer el personal (peritos o fuerzas de la ley o sede judicial) que resguardará la evidencia.
  - Ubicar el material recolectado respetando temperatura, humedad, movimientos indebidos, golpes.
  - Cadena de custodia.

Como corolario a la labor anterior, la cadena de custodia de los elementos preservados es un estándar importante también para obtener la admisibilidad de una prueba digital. No solo hace falta al detalle minucioso y certero de los elementos secuestrados sino también al pasaje o derrotero que han tenido los mismos hasta llegar a manos del investigador.

Una definición a mi entender contundente reza que una cadena de custodia "*es el conjunto de medidas que deben adoptarse a fin de preservar la identidad e integridad de objetos o muestras que pueden ser fuente de prueba de hechos criminales, para su total eficacia procesal*".

Elementos tales como los que se enuncian a continuación despliegan una correcta integración de la cadena de custodia:

- Identidad de las personas actuantes.
- Fecha, hora y lugar donde se efectúa la incautación de los efectos.
- Registro de testigos que presencien la tarea con invitación a firmar el acta.
- Descripción detallada de lo incautado y las tareas realizadas.
- Sellado de la evidencia una vez finalizada la labor.
- Destino de los objetos incautados.

Si la evidencia cambia de destino, se hará lo que a continuación se describe:

- Registrar unidad de origen y destino.
- Descripción de los elementos que se envían.
- Fecha y hora del movimiento.
- Nombre y firma de quien recibe y entrega.
- Estado de la evidencia.
- Motivo por el cual se envía la evidencia.
- Forma de traslado.

IV - LA PRÁCTICA DE LA PERICIA INFORMÁTICA

En párrafos anteriores se mencionó que la pericia informática puede recaer sobre hechos informáticos, ya sean producidos por el usuario o generados por el propio sistema operativo.

Se puede solicitar a los expertos que viertan sus opiniones sobre mensajería de datos, páginas web, en cuanto a sus estructuras, los elementos contenidos en los mismos y el origen, de los cuales podrá determinar su existencia, veracidad, presencia en la nube y demás elementos que compongan el análisis de las evidencias digitales.

Existen elementos digitales que, por utilización masiva, en hechos delictivos o no ameritan análisis técnicos especiales.

1. Tesis sobre un *email.* Todo está en los detalles

El correo electrónico, comúnmente llamado *email*, es un elemento de vital importancia como fuente de comunicación entre dos entidades: *una emisora* (que envía el correo)

y *una o dos receptoras* (quien o quienes reciben el correo). Es factible que muchos de esos correos presenten adjuntos en su composición.(1)

La experticia a realizar en un correo electrónico debe hacerse sobre la computadora que generó ese correo y en las computadoras de quienes lo recibieron.

Los datos que analiza sobre el mismo se refieren precisamente a sus datos ocultos, comúnmente denominados *metadatos*(2). La realización de un análisis detallado de dirección IP del remitente del correo, el programa utilizado para realizar el envío del correo y el proveedor de servicios de Internet es una labor que debe realizarse en todo análisis de un correo electrónico. Los metadatos se detallan en las *cabeceras o encabezados* que posee todo correo electrónico.

La buena práctica establecida aclara que dicho análisis es menester realizarlo en ambos canales que han servido para el intercambio del correo: *receptor y emisor/es*, y sin dejar de lado la verificación de los servidores de correo electrónico, generalmente provistos por un proveedor de servicios de Internet, para analizar si el correo en cuestión ha generado registros o *logs*(3) en aquellos.

Nuevamente, las cabeceras o encabezados serán los repositores de todos los datos que a modo de bitácora se registren en los servidores.

Es importante saber si es posible determinar la existencia de una casilla de correo electrónico. No se puede hablar de una casilla de correo falsa o inventada sino solo de existencia. Sí se puede hablar de una casilla con datos falsos cuyo propietario haya querido esconder su verdadera identidad con fines no precisamente dignos.

Existen aplicaciones comerciales y consultas a sitios web que permiten determinar la existencia de una casilla de correo electrónico. En el caso de una empresa, el administrador del servidor puede suministrar datos de los usuarios que posean casillas de correo corporativas.

Las casillas de correo electrónico no poseen titularidad. No son objetos de pertenencia a un humano que la utiliza. Pueden ser consideradas espacios en discos rígidos que brindan sendos proveedores -públicos o privados- para que un usuario pueda mantener intercambio electrónico con otro. A modo coloquial, una casilla de correo se presta.

En los proveedores públicos de servicios de correo electrónico, tipo Yahoo! o Hotmail, por la misma condición de ser públicos, ofrecen a sus usuarios total privacidad y muchas veces los datos de registración pueden ser falsos, ya que no hay acreditación fidedigna de que el usuario que creó la cuenta *es quien dice ser*.

2. Labores sobre sitios o páginas web

Cada sitio web, que descansa en la *nube*, posee un único identificador de dominio que puede ser asignado a una persona física o eventualmente jurídica.

(1) Orta Martínez, Raymond J.: "Capítulo Primero - Las pruebas en el derecho informático" en Rico Carrillo, Mariliana (Coord.): "Derecho en las nuevas tecnologías" - Ediciones La Rocca - 2007 - pág. 567

(2) Metadato: dato del dato. Los documentos informáticos poseen esta virtud por la cual se pueden obtener datos sensibles como ser: fecha de creación, tamaño, fecha de modificación y autor. En el caso de los correos electrónicos, se le adiciona la dirección IP de origen (si procede), que tiene un valor de importancia en pericia informática sea forense o no

(3) *Log* (informática). En informática, se usa el término *log*, historial de log o registro a la grabación secuencial en un archivo o en una base de datos de todos los acontecimientos (eventos o acciones) que afectan a un proceso particular (aplicación, actividad de una red informática, etc.)

La registración de un dominio para presencia en Internet posee varios requisitos para su asignación, siendo el más importante los datos de contacto de la persona que lo efectúa. Existen distintos sitios web fuera de la Argentina que brindan información relevante sobre los dominios y su historial de presencia y datos de registración. Son un verdadero elemento probatorio a la hora de ser utilizados como prueba, sobre todo en sitios que contienen material pornográfico o cualquier otro delito grave.

Otro elemento que no debe escapar al investigador informático forense es el análisis del denominado *código fuente*(4) del sitio web objeto de experticia, ya que dicho código fuente puede ser copiado por otros sitios web. Es por ello que se podría cometer el delito de violación de derechos intelectuales o también, en dicho código, puede encontrarse inmerso un código malicioso que represente un posible ataque al usuario que ingresa al sitio web infectado o lo redirige a otro sitio. *La seguridad por oscuridad* implica que un usuario ingresa a un sitio de pornografía de adultos, intencionalmente o no, y se lo redirige a un espacio de pornografía infantil, código fuente "oculto" en el código fuente.

3. Una imagen, un documento valen más que mil palabras

Un programa informático, cuando es utilizado por el usuario, genera un documento que se denomina "archivo". Esto es un procesador de texto, de tipo *Word*, que forma parte de la familia de Microsoft Office (como paquete de productividad), que genera un documento con la extensión *.doc*. Generalmente, todos los archivos con esta extensión se asocian a procesadores de texto, como los archivos de imágenes se asocian a extensiones *.jpf* o *.tiff*(5), los cuales se abren con programas editores de imágenes o fotografías.

Estos archivos, que son generados por el usuario con utilización de una herramienta informática, suelen guardar información relevante en sus metadatos, que pueden ser asociados al propietario de la computadora. Para la práctica forense, la obtención de los metadatos es de importancia capital.

4. Con licencia para utilizar

La mayor parte de los programas instalados en computadoras poseen una licencia de uso provista por su creador para que el mismo pueda ser utilizado.

Esas licencias son legalmente comerciales y con un coste de acuerdo con sus versiones. Básicamente, cuando se instala un software en una computadora se necesita una clave de acceso provista por su fabricante dentro del CD de instalación o a través de una instalación vía web.

Existen, sin embargo, formas de ejecutar programas sin las licencias de uso, ya sea bajando los mismos desde sitios web de Internet o adquiriendo CD o DVD apócrifos en lugares que se dedican al comercio ilegal de productos de *software*.

El sistema operativo de una computadora posee varios archivos propietarios que registran toda la información del usuario que está instalando el *software* y suelen preservarse en archivos -muchas veces- ocultos a la visión del usuario.

(4) El código fuente es una serie de instrucciones o líneas de código que permiten ejecutar un programa informático. Es una programación imperativa, ya que dichas líneas emiten órdenes a la computadora en pro de un resultado, por ejemplo, la ejecución de un cálculo y luego que se emita una salida por impresora

(5) .jpg - .tiff: son estándares que identifican archivos de imágenes y su tipo de compresión

Esta información es de suma importancia, por cuanto aquellos programas que se instalan (ya sea procesadores de texto, planillas de cálculo o *software* para diseño gráfico), luego de que se haya instalado el sistema operativo, arrastran en sus metadatos información parcial o total del propietario del equipo informático, que pueden servir a una investigación forense.

V - "CADA CONTACTO DEJA UN RASTRO"(6). ARTEFACTOS DE WINDOWS

El sistema operativo Windows es, a mi entender, el más común en cuanto a su utilización por los usuarios, dado su interfaz gráfica y amigable que hace su manejo más intuitivo.

Este sistema operativo, tan cuestionado pero que ha avanzado tecnológicamente, es un excelente repositorio de elementos que son analizados desde el punto de vista forense, y que pueden llegar a contener información de relevancia. Esos elementos se denominan *artefactos*.

Estos artefactos suelen ser contenedores de pistas o trazas de actividades que no son visualizadas a simple vista, sino con un *software* forense -comercial o libre-, obteniendo buenos resultados, incluso con elementos que hayan sido inicialmente eliminados.

A continuación, se detallan los artefactos más relevantes y cuál es la información de utilidad que puede ser encontrada:

1. Archivos de *logs* o archivos del sistema

Estos *archivos de logs* pueden contener, en forma detallada, acciones y errores producidos en un proceso de instalación, una actualización de un *software* o cualquier otro proceso dentro del sistema operativo. Una investigación en estos archivos podría determinar, por ejemplo, un acceso indebido realizado por un atacante a un servidor.

2. El registro de Windows

El *registro de Windows* es una base de datos dentro del propio sistema operativo que guarda las configuraciones básicas del sistema operativo de mención así como también datos de programas, dispositivos, *hardware* y usuarios del equipo.

Es interesante saber que este registro suele guardar entre sus carpetas información tal como casillas de correo electrónico que se crearon, dispositivos periféricos que se conectaron mediante puertos USB, archivos instalados y, eventualmente, contraseñas de acceso a determinados formularios de páginas web e incluso de acceso a redes sociales.

(6) Principio de Edmond Locard: el principio de intercambio de Locard es un concepto que fue desarrollado por el doctor Edmond Locard (1877-1966). Locard especuló que cada vez que se hace contacto con otra persona, lugar o cosa, el resultado es un intercambio de materiales físicos. Él creía que no importaba a donde vayan los criminales o lo que hagan los criminales, estando en contacto con cosas, dejan todo tipo de evidencia, incluyendo ADN, huellas, cabellos, células de piel, sangre, fluidos corporales, piezas de vestimenta, fibras y más. A la misma vez, ellos toman también algo de la escena

3. La papelera de reciclaje

La *papelera de reciclaje*[7] no es ni más ni menos que un archivo o carpeta del sistema donde el sistema operativo resguarda aquellos archivos que fueron eliminados por el usuario.

Vale decir que los archivos que se eliminan de la papelera, en realidad, corren una suerte de desconexión y no visualización, pero siguen ocultos en algún sector del disco investigado.

Con herramientas de *software* y de búsqueda adecuada es posible reconstruir el archivo eliminado y presentarlo dentro de un informe técnico si su recupero es importante. Como corolario a esta afirmación, se informa que mediante dichas herramientas se puede obtener adecuadamente la fecha en que fue eliminado un archivo y la ubicación que podría haber tenido en el disco.

4. Archivos de impresión

Imprimir un archivo[8] desde una computadora genera una suerte de cola de impresión, donde los archivos se van encolando hasta poder, finalmente, ser impresos.

En dicha cola de impresión se crean archivos temporales que registran internamente el archivo que concretamente debería imprimirse. Esos archivos temporales son de extensión *.spl* y *.shd*. Este último archivo temporal guarda metadatos como ser: propietario del equipo que está imprimiendo el archivo, nombre del archivo que se imprime, formato de impresión y datos de la impresora. Los archivos temporales son eliminados una vez finalizado el proceso de impresión.

En toda investigación forense informática, no debe descartarse este tipo de búsqueda dentro de los elementos eliminados en una computadora, ya que se puede obtener información de utilidad sobre lo último que se imprimió y datos sensibles del equipo e impresora.

Existen otros artefactos de Windows que son susceptibles de investigación, de ser necesario; ellos son:

- *Mac times*: son artefactos que indican cuándo se creó, modificó o eliminó un archivo de una computadora. Las *mac times* son de vital importancia para evaluar las veces que se pudo modificar un archivo y si existen constancias de la modificación realizada.
- *Los archivos prefetch*: son archivos generados por el sistema operativo cuando se ejecuta un programa. Una vez hecho esto, ese archivo ejecutado se coloca en la carpeta *prefetch*, de manera tal que la próxima vez que se necesite ejecutar un programa, el sistema operativo busca el mismo en la carpeta *prefetch* y de no encontrarlo los busca en la ruta que tiene asignada.

La utilidad de estos archivos es acelerar procesos de ejecución de dicho programa y tener una noción de cuáles son los archivos que tienen una ejecución sostenida dentro de ese equipo (por ejemplo, un editor de imágenes).[9]

(7) Sheldon, Bob: "Forensic analysis of windows system", en Eoghan, Casey (Ed.): "Computer crime investigation - Forensic tools and technology" - Academic Press - London-California - 2002 - pág. 145

(8) Sheldon, Bob: "Forensic analysis of windows system", en Eoghan, Casey (Ed.): "Computer crime investigation - Forensic tools and technology" - Academic Press - London-California - 2002 - pág. 145

(9) La ejecución sostenida de un archivo como el editor de imágenes hace suponer *a priori* que su usuario modifica o altera, reiteradamente, imágenes o fotografías

Los artefactos mencionados son susceptibles de investigación y análisis. Por eso, el investigador no debe apartarlos de la bitácora de consulta.

VI - INVESTIGANDO LA NUBE

En toda investigación forense no solo nos adentramos en las búsquedas de información relevante dentro de dispositivos digitales, sino también ascendemos al espacio virtual, llamado actualmente *nube o cloud*, donde se encuentran redes sociales y la web profunda.

Cabe aclarar que, al ser la nube un espacio virtual, existe un enfoque de investigación tecnológica oportuna pero también hay un aspecto legal en el cual los investigadores forenses tenemos una limitación. Mucha de la información contenida en redes sociales o sitios web es privada y para obtenerla se deben solicitar oficios ordenados por un juez federal, y si los sitios sospechados son foráneos, los oficios serán internacionales.

Sin duda, nuestra labor técnica no hace más que reafirmar evidencias o propiciarlas al procedimiento para que el operador judicial, frente a una denuncia, empiece su labor investigativa.

Un elemento importante a todo evento en la nube es la preservación de las evidencias, que se observan utilizando herramientas o *software* específicos para darle a las mismas verdadera existencia. La participación de un notario puede ser de utilidad, quien aportará el informe del experto informático a su acta notarial.

1. Seis grados de separación

La aparición de las redes sociales ha generado en el ser humano una suerte de fenómeno social muy pocas veces igualado. Facebook, Twitter, LinkedIn y otras permiten establecer relaciones personales entre usuarios, pudiendo compartir material (archivos o imágenes), pensamientos o reflexiones de su vida íntima. No es extraño encontrar en estas redes que sus usuarios vuelcan su dolor o alegría, así como también el relato de un viaje o la adquisición de algún bien.

La teoría de los *seis grados de separación* intenta *probar que cualquier persona en la Tierra puede estar conectada a otra a través de una cadena de conocidos que no tiene más de cinco o seis intermediarios*.(10)

Esto es aplicable a las redes sociales actuales, donde un usuario tiene un número importante de contactos que en realidad provienen de un contacto generador y muchas veces no se conocen o no comparten gustos o afinidades.

Pero no todo lo que reluce es oro y no todo lo que se muestra en las redes es información grata. Muchas veces, estas redes han sido usadas con fines complejos, como ser pornografía o pedofilia, porno venganza o difamación de algún usuario. Para estos casos y en el supuesto que se deba denunciar un ilícito, se deben tener presente aspectos esenciales tales como: la validación de los usuarios agresores (poseen un ID identificatorio), la captura de evidencia del contenido que se observa en la pantalla, identificando, validando y registrando las evidencias electrónicas mediante protocolos o buenas prácticas establecidas.

(10) Delbono, Patricia M.: "Seis grados de separación" - Revista Coordenadas - Copitec - N° 100 - abril/2015 - año XXIX - pág. 8

Dado que las relaciones dentro de las redes sociales son cambiantes o pueden desaparecer, se debe gestionar la posibilidad de preservar la evidencia digital con la actuación de un notario que brinda un marco legal de primer nivel a la labor del experto informático.

Si alguna de las premisas comentadas no es cumplida en forma correcta, se podrían impugnar las evidencias presentadas y con ello se perderían las pruebas que respaldan el caso.

2. Alerta en lo profundo. La *deep web* o web invisible

No solo se puede navegar por Internet a través de los navegadores convencionales, como Firefox, Chrome o Internet Explorer y con los que se puede obtener variado tipo de información, generalmente indexada y muchas veces reiterativa, que se denomina *surface web o web superficial*.

La llamada *deep web, dark web o web invisible* es parte del contenido de Internet al que no se puede acceder por los motores de búsqueda convencionales, como ser Google, Yahoo!, Bing o DuckDuckGo, ni por los navegadores clásicos, ya nombrados más arriba.

Cuando se navega por los navegadores convencionales, nuestras visitas son rastreadas a través de nuestra dirección IP, la cual es provista por nuestro proveedor de servicios de Internet. En contraposición, navegar por la *deep web* es prácticamente anónimo y nuestras visitas no son rastreadas.

Navegar por la web profunda nos permite adentrarnos en un mundo muchas veces peligroso y carente de seguridad, sobre todo para los inexpertos internautas. El material suele ser variado, desde pornografía infantil hasta narcotráfico, pasando por sicarios, hackers y personas que limpian antecedentes penales. La moneda de uso corriente es el *bitcoin*.

Las páginas web en la navegación *surface* son www.unapagina.com; en cambio, en la *deep web* el formato luce como *asd67asdt124byasdfyieerbhi34y8 (punto) onion* y están encriptadas.(11)

La aplicación de primer nivel para navegar por la *deep web* se denomina *tor o red tor*(12). Este navegador utiliza la privacidad optimizada de Mozilla Firefox y es un *software* de *código abierto*(13), que le permite al usuario navegar en forma anónima, ya que oculta su dirección IP. Puede acceder a sitios web potencialmente bloqueados y, lo más resaltante, no rastrea al usuario.

Investigar elementos delictivos en una red *tor* no es tarea sencilla. Si bien el sitio en cuestión tiene innumerables contenidos con material potencialmente susceptible de incurrir en delito, su comprobación no es fácil, máxime cuando se debe hallar *el humano detrás del teclado*. Realizar una tarea de inteligencia en esta red implica la aparición del agente encubierto, una figura no siempre aceptada en el ámbito judicial.

(11) Internautas 21 - ¿Qué es la *deep web*? Videos reales e imágenes
Chema Alonso - De paseo por la *deep web*

(12) *Tor project - Privacy online*

(13) Código abierto. Un *software* que posee código abierto (también llamado *open source*) implica que puede ser utilizado sin adquirir una licencia comercial. Su propietario permite a los usuarios utilizar, cambiar y redistribuir el *software* a cualquiera, para cualquier propósito, ya sea en su forma modificada o en su forma original

No habría, en principio, otra alternativa de detectar delincuentes en *tor*. Además, se debe conocer profundamente la forma de navegar profundamente y evaluar si los potenciales delincuentes cometen algún error, por lo cual dejan al descubierto su identidad.

3. Investigación en la nube utilizando fuentes abiertas. "La información es poder"

El término *fuentes abiertas* u *osint*[14] se refiere a toda la información que aparece publicada en Internet y abierta al público. Esa información se caracteriza por ser caótica, desordenada y desclasificada, y por permitir tomar decisiones a quien encargó la investigación.

El vocablo "*int*" no solo se asocia a *osint*, sino a otras formas de realizar inteligencia, las cuales son:

- *Humint*: son fuentes de información generada a través de humanos.
- *Sigint*: fuentes de información obtenidas de elementos digitales.
- *Geoint*: estas son las informaciones que provienen de satélites.

Para realizar investigación con fuentes abiertas, no solo sirve conocer cuáles son las fuentes que se utilizan, sino también poder encontrarlas. Casi como derivación del punto anterior donde se explicó lo que es la navegación profunda y sus peligros, las fuentes de investigación potencialmente útiles se encuentran en la *deep web* y también en la *web superficial (surface web)*.

Otro elemento que debe tener el investigador es que muchas herramientas son gratis, pero otras pagas, no todas las herramientas obtienen información a nivel local y solo pueden ser utilizadas foráneamente.

Como se ha mencionado, la información que se obtiene es caótica y desclasificada, siendo el investigador el que debe darle, con su experiencia, un enfoque práctico y certero para futuras *decisiones*.[15]

VII - CONCLUSIÓN

No existe prácticamente actividad cotidiana que no incorpore en su desarrollo algún recurso digital o informático. Se dice que todo medio digital asociado al humano es una prolongación de su vida, donde se refugian eventos personales y profesionales, y por qué no delictivos, dependiendo de la idiosincrasia del individuo.

Las pruebas informáticas pueden plantarse sobre prácticamente cualquier recurso digital, donde la habilidad del investigador y el conocimiento de sus herramientas informáticas darán un resultado exitoso a lo que se investiga, proveyendo al juzgador o a quien solicita una investigación suficientes elementos para decidir sobre una causa o proceso judicial.

(14) *Osint* es un término anglosajón y se refiere a *open source intelligence* o inteligencia de fuentes abiertas

(15) Bazzell, Michael: "Hiding from the internet: eliminating personal online information" (*e-book*)
Bazzell, Michael y Justin, Carroll: "The complete privacy & security desk reference"

Toda labor de investigación sobre medios digitales está suscripta a lo que se buscará y la manera de buscarlo. Ambas premisas (qué y cómo) incidirán en los tiempos de proceso, resultados de las búsquedas y un informe concluyente.

Dicen que "la información es poder", pero la información contenida en medios digitales es estrechamente más poderosa. Por ello, se debe preservar su integridad, disponibilidad y confidencialidad, que son los paradigmas de la seguridad de la información.

CIBERCRIMEN Y EVIDENCIA DIGITAL: PROBLEMÁTICA PROBATORIA

Federico A. Borzi Cirilli(*)

I - NOCIONES PRELIMINARES

En nuestros días es inimaginable una sociedad sin Internet, correos electrónicos, motores de búsqueda, aplicaciones, mensajería instantánea, redes sociales, etc., por lo que estas tecnologías de información y comunicación (TIC) se filtran inevitablemente en todos los espacios de nuestra vida y, por supuesto, muchas veces nos causan -o causamos mediante ellas- distintas clases de daños, algunas veces involuntarios y otras intencionales.

Inicialmente, los riesgos creados mediante la informática no eran relacionados con la órbita del derecho penal, y se encuadraban genéricamente como derecho informático, el cual ha sido definido por Kemper como "*aquella parte del Derecho de la Información que regula el tratamiento automatizado de la información*"(1), y es luego el derecho de daños, a través del artículo 1113 del derogado Código Civil de Vélez Sarsfield, el receptor legal de dichos conflictos.

Paulatinamente, y con la explosión tecnológica aún en curso, se fueron intensificando las consecuencias negativas del uso de estas tecnologías, y se comenzó a acudir al derecho penal a fin de paliarlas, desarrollándose definiciones como la esbozada por Rodríguez Hauschildt, quien definió al delito informático como "*cualquier delito que involucre el procesamiento o transmisión automática de datos*"(2). A esa altura no se consi-

(*) Abogado (UBA). Especialista en derecho penal (UBA/CASI). En ejercicio independiente de la profesión en el fuero penal ordinario nacional, provincial y federal. Autor de numerosas publicaciones en temas de derecho penal y procesal penal

(1) Kemper, Ana M.: "Nuevas tecnologías y función notarial" - Ed. Ut Supra - Bs. As. - 2009 - pág. 17

(2) Rodríguez Hauschildt, Victoria M.: "Derecho informático" - 1ª ed. - Ed. Aplicación Tributaria - Bs. As. - 2007 - pág. 48

deraba que estos delitos constituyeran una categoría nueva sino una nueva modalidad para cometer viejos delitos. Como se dijo en el proyecto que desembocara en la ley 26388 -que incorporó la casi totalidad de los delitos informáticos que se encuentran legislados en nuestro ordenamiento-: "*No nos encontramos en presencia de nuevos bienes jurídicos a ser tutelados por la ley penal, sino que se trata, en general, de nuevas formas de ataque a los bienes jurídicos tradicionales…*" (Expte. 5864-d-2006).

Sin embargo, fundamentalmente en esta última década, se fueron delineando, tanto a través de elaboraciones doctrinarias como de regulaciones legales, categorías delictivas específicas de criminalidad informática como los denominados *grooming, phishing, cybrebullying, sexting, cyberstalking*, interferencia con el correo electrónico, acceso ilegal a un sistema de información, delitos en relación con la protección de datos, delitos que protegen la integridad de los sistemas, estafa informática, etc.(3)

En este trabajo abordaremos lo relacionado con las problemáticas probatorias en este tipo de delitos, primero de un modo general y luego a través de aspectos puntuales referidos a determinados tipos penales.

II - DELITOS INFORMÁTICOS EN NUESTRO ORDENAMIENTO

Antes de continuar debemos efectuar una somera enumeración de los delitos informáticos incorporados a nuestro ordenamiento a través de la recién citada ley 26388, así como de la ley 26904, a fin de poder delimitar el campo de trabajo. En ese sentido, los delitos informáticos legislados en nuestro ordenamiento jurídico son los siguientes:

- ofrecimiento, distribución y tenencia de imágenes relacionadas con pornografía infantil [art. 128 del Código Penal (CP)];
- violación de secretos y privacidad: violación de correspondencia electrónica (art. 153, CP), acceso ilegítimo a un sistema informático (art. 153 bis, CP), publicación abusiva de correspondencia (art. 155, CP), revelación de secretos (art. 157, CP), delitos relacionados con protección de datos personales (art. 157 bis, CP);
- defraudación informática [art. 173, inc. 16), CP];
- daño informático (arts. 183 y 184, CP);
- interrupción de comunicaciones electrónicas (art. 197, CP); y
- destrucción, alteración o inutilización de medios de prueba (art. 255, CP)
- *grooming* (art. 131, CP).

III - ¿QUÉ ES LA EVIDENCIA DIGITAL?

Ahora bien, encontrándonos ya introducidos en el tema, pasemos a enfocar la atención en lo atinente a la prueba. Debemos recurrir, preliminarmente, a la modificación que se le efectuara al artículo 77 del CP, en lo que tiene que ver con lo que abarcan ahora los conceptos "documento", "firma" y "certificado". Así, se encuentra ahora establecido legalmente que el término "documento" comprende toda representación de actos o hechos,

(3) Sueiro, Carlos C.: "Casos de criminalidad informática y prueba digital" - Ed. Ad-Hoc - Bs. As. - 2017 -, con anexo con cita de Informe General de la Asociación Internacional de Derecho Penal (AIDP); Riquert, Marcelo A.: "Convenio de Cibercriminalidad de Budapest y Mercosur en Derecho Penal" - Infojus - N° 7 - Bs. As. - 2014 - año III - págs. 107/80

con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión. Los términos "firma" y "suscripción" comprenden la firma digital, la creación de una firma digital o firmar digitalmente. Los términos "instrumento privado" y "certificado" comprenden el documento digital firmado digitalmente.

Los conceptos de cada uno de ellos fueron abordados por la ya citada Kemper, quien refiere que el documento electrónico en sentido amplio es el "*…gestado con intervención de una computadora a través de sus propios órganos de salida (monitor, impresora, etc.), cuya característica es que son perceptibles y con textos alfanuméricos legibles directamente por el hombre sin necesidad de intervenciones por parte de máquinas traductoras*". Mientras que, en sentido estricto, "*es el documento elaborado por el propio hardware, conforme al sistema utilizado y programa establecido, que desde su creación hasta su archivo permanece sin haber salido del contexto de su origen*".

En lo que tiene que ver con la firma digital o electrónica, que como veremos no son sinónimos, explica la autora que la primera es una herramienta tecnológica que permite garantizar la autoría e integridad de los documentos digitales, posibilitando que estos gocen de una característica que únicamente era propia de los documentos en papel. Como adelantábamos, ambos términos no poseen el mismo significado: "*en el caso de la firma digital existe una presunción* iuris tantum *en su favor; esto significa que si un documento firmado digitalmente es verificado correctamente se presupone, salvo prueba en contrario, que proviene del suscriptor del certificado asociado y que no fue modificado. Por el contrario, en el caso de la firma electrónica, de ser desconocida por su titular, corresponde a quien la invoca acreditar su validez"*. Por su parte, los certificados digitales son pequeños documentos digitales que dan fe de la vinculación entre una clave pública y un individuo o entidad, y contienen una clave pública y un nombre, así como una fecha de expiración, el nombre de la autoridad certificante y un número de serie.(4)

Como estas temáticas suelen ser un tanto hostiles para aquellos que nos dedicamos a las ciencias sociales, puntualmente a los letrados y auxiliares de la justicia, cabe emparentar el sistema utilizado por la justicia nacional y federal con el caso de la firma electrónica, mientras que el utilizado por la justicia provincial (a través de los denominados "token") trataría de firmas y certificados digitales.

Como refiere Lombardo: "*el objetivo que ha perseguido esta normativa ha sido, sin duda alguna, adaptar las nuevas técnicas, modalidades y avances tecnológicos a las disposiciones penales consagradas como ilicitudes dentro de nuestro cuerpo de leyes. En síntesis, se ha elevado a la categoría jurídica de cosa o documento a los sistemas y programas informáticos como también a las comunicaciones electrónicas, con el objeto de sancionar de igual manera las ilicitudes cometidas a través de estos medios, con estos objetos o contra estos bienes*".(5)

IV - PROBLEMAS PROBATORIOS DE CRIMINALIDAD INFORMÁTICA

a) Un abordaje general

Como podrá observarse, el nuevo campo de trabajo aparece en escena con sus propias vicisitudes probatorias. Ante todo cabe recordar que en el derecho penal y

(4) Kemper, Ana M.: "Nuevas tecnologías y función notarial" - Ed. Ut Supra - Bs. As. - 2009 - pág. 51

(5) Niño, Luis: "Delitos contra la propiedad" - Ed. Ad-Hoc - 2011 - pág. 1055

particularmente en el derecho procesal penal rige el principio de libertad probatoria en virtud del cual, como es bien sabido, los hechos investigados pueden acreditarse recurriendo a todo tipo de elementos de convicción, siempre y cuando no se vulneren garantías constitucionales de los involucrados.

Como explica Sueiro en su libro sobre casos de criminalidad informática: "*si bien a la fecha no se ha realizado una reforma en materia de criminalidad informática a nivel del Código Procesal Penal de la Nación, lo cierto es que cada vez más ella resulta imperiosa, indispensable y necesaria, debido al desplazamiento gradual en los procesos penales, de la prueba física, corpórea o tangible hacia la prueba digital, electrónica o intangible*".(6)

Es que nos encontramos con nuevas modalidades investigativas que se van creando y adaptando a modo de espejo con las modalidades delictivas; lamentablemente, esta circunstancia hace que aquellas siempre vayan detrás de estas. Es así que ahora las tareas de inteligencia habituales en cualquier investigación se traducen en "ciberpatrullajes" y nos encontramos ante la necesidad de identificar computadoras, celulares e inspeccionar *smartphones*, entre otros dispositivos en constante evolución y cambio.

En el mismo sentido, se suelen presentar grandes inconvenientes en torno a la debida acreditación de los tipos subjetivos, sin la cual mal podrían castigarse este tipo de conductas. Ya nos advertía el citado Lombardo al respecto: "*la complicación, en la praxis, de perseguir penalmente a quienes introdujeran en el comercio una herramienta potencialmente dañosa, ya que resultará sumamente dificultoso acreditar la existencia del dolo específico que la figura exige*".(7)

También es cierto que la utilización de servicios como Google Maps, correos electrónicos, fotografías de pantallas y, las ya en este contexto resultan antiguas -grabaciones de audio y/o video en CD, DVD o USB, o sus respectivos fotogramas-, sirven muchas veces como pruebas cruciales para el descubrimiento de ciberdelitos.

Un aspecto no menor cuando hablamos de cibercrimen es el relativo a la conservación de la evidencia digital, de naturaleza muy distinta -como es obvio- a la tradicional. En un proceso penal donde se investigaba la comisión del delito de daño informático que habría sido cometido por ex empleados de un banco, recientemente la Cámara de Apelaciones en lo Penal, Contravencional y de Faltas de la Ciudad Autónoma de Buenos Aires, a través de su Sala II, resolvió la nulidad de la intervención de quien fue llamado por el Ministerio Público Fiscal a realizar valoraciones en carácter de perito elaborado por la empresa de la que había sido responsable ("N. N. s/ infr. art. 184, inc. 6), CP" - 4/4/2017).

El hecho de que nos encontremos en la práctica, por ejemplo, con casos de memorias inutilizadas por descargas por no utilizarse el brazalete de descarga a tierra correspondiente, el inadecuado precinto de celulares o la falta de conservación de otras pruebas digitales por falta de copias adecuadas -esto sucede afortunadamente cada vez con menor frecuencia- se presentan muchas veces como obstáculos al avance de los procesos ya que suelen constituir el cauce principal de prueba.

Salta a la vista que los desafíos que el cibercrimen nos plantea como operadores judiciales no son menores, obligándonos día a día a realizar grandes esfuerzos para estar a la altura de los tiempos que corren, ya sea que nuestra función sea construir una imputación o, por el contrario, contrarrestar una acusación mediante contrapruebas y

(6) Sueiro, Carlos C.: "Casos de criminalidad informática y prueba digital" - Ed. Ad-Hoc - 2017 - pág. 21

(7) Niño, Luis: "Delitos contra la propiedad" - Ed. Ad-Hoc - Bs. As. - 2011 - pág. 1060

estrategias defensistas. Por ejemplo, casos de tecnologías de doble uso, de acciones automáticas por parte de sitios de Internet o los de estenografías -dibujos ocultos en los que al hacer click se activan y permiten descubrir el oculto debajo del original-, todos ellos abordados por el citado Sueiro en su libro de casos prácticos, nos enfrentan con dilemas en torno a la persecución de los casos ilícitos sin coartar el uso lícito de las nuevas tecnologías. En tales casos, el desafío será tratar de permitir la existencia de estas herramientas y solamente sancionar su uso en casos concretos, es decir, cuando se halle un encuadre jurídico penal en alguno de los tipos mencionados en el punto II de este trabajo.

b) La dirección IP como medio de prueba

Un reciente fallo de la Sala I de la Cámara Federal de Casación Penal nos permitirá abordar la importancia de la dirección IP como medio de prueba en los ciberdelitos. Esta causa se inició por una denuncia del presidente y representante legal de una cooperativa a una persona -que fue contador en la misma y se desvinculó en malos términos de esta- por haber ingresado en forma ilegal al sitio web de la AFIP con las claves fiscales del denunciante y de la cooperativa mencionada, con el fin de generar deudas en los registros mediante declaraciones juradas que no se correspondían con la realidad ni con el giro contable de la cooperativa.

En primera instancia, el Juzgado Federal 2 de San Isidro condenó al acusado por acceder de un modo ilegítimo a un sistema informático de acceso restringido, en violación del artículo 153 bis, CP ya que, luego de su desvinculación de la cooperativa, no contaba con autorización para acceder al sistema, el cual requería de una clave fiscal, y sin embargo ingresó con el fin antes señalado. El condenado recurrió la sentencia en casación argumentando que no se había acreditado fehacientemente que fuese el autor del delito, y que su titularidad de la dirección IP vinculada a los accesos no servía para acreditar su actividad personal. Ante ello, Casación confirmó la condena, entendiendo que sí se había probado su accionar y la comisión del delito porque la prueba informática de la IP no fue un indicio aislado, sino que estaba enmarcado y respaldado por todo un plexo probatorio que incluía la información relacionada con el servicio de Internet utilizado para acceder a la página web de la AFIP: la renuncia de G.W.R, las declaraciones de su ex empleador y el hecho de que conocía las claves fiscales necesarias debido a su desempeño como contador.(8)

En otro caso, que involucra a un estudiante universitario de ingeniería en sistemas que, a través de un IP situado en el extranjero, realizó en el país una transferencia indebida de dinero entre cuentas bancarias, Casación confirmó su condena por el delito de defraudación mediante técnicas de manipulación informática en calidad de autor -*phishing*-. Más allá de la incapacidad técnica invocada por la defensa, pues esta no se corresponde con las tareas que desempeñaba a favor de su empleador ni con su carácter de estudiante universitario de ingeniería en sistemas, está presente la relación lógica necesaria entre las distintas piezas probatorias, a través de las cuales se pudo averiguar que había sido aquel quien, mediante manipulaciones informáticas, había extraído indebidamente fondos de la cuenta bancaria del damnificado.(9)

(8) Ranieli, Germán Walter s/violación sist. informático - art. 153 bis, primer párrafo" - CFed. Casación Penal - Sala I - 30/3/2017

(9) "C., P. A. s/recurso de casación" - CFed. Casación Penal - Sala III - 16/6/2015

Cabe señalar, como explica Vaninetti -a quien seguimos en este punto-, que la IP (técnicamente Internet Protocol -Protocolo de Internet-) es un conjunto de números (cuatro números decimales, separados por un punto entre sí) que identifican la interfaz de un dispositivo (una computadora, *smartphone* etc.) dentro de una red que utilice el Protocolo IP (*Internet Protocol*). La existencia de la IP se debe a que la información que circula en la red necesita saber por dónde debe hacerlo y dónde tiene que ir. Pueden existir dos tipos de IP: una estática (es única y siempre la misma) o dinámica (cambia al reconectarse). Un proveedor de acceso a Internet que tiene un contrato con un abonado a Internet normalmente mantiene un fichero histórico con la dirección IP (fija o dinámica) asignada, el número de identificación del suscriptor, la fecha, la hora y la duración de la asignación de dirección. De igual modo, si el usuario de Internet está utilizando una red pública de telecomunicaciones, como un teléfono móvil o fijo, la compañía telefónica también registrará el número marcado, junto con la fecha, la hora y la duración, para la posterior facturación.(10)

El Superior Tribunal Español se ha expedido en el sentido de que la IP no es ni más ni menos que un indicio que deberá reforzarse con un plexo probatorio -testimoniales, pericias, documental, informes, etc.- ya que ser "*…usuario de un ordenador y titular de la línea telefónica no lleva necesariamente a la conclusión de que esa persona sea responsable de toda la utilización telemática de su línea*" (STS 8316/2012, España). Como explica Cafferatta Nores(11), la eficacia probatoria de toda prueba indiciaria dependerá, en primer lugar, de que el hecho constitutivo del indicio esté fehacientemente acreditado. En segundo término, del grado de veracidad, objetivamente comprobable, de la enunciación general con la cual se lo relaciona con aquel. Por último, de la corrección lógica del enlace entre ambos términos.

En definitiva, y sin perjuicio de que, como advierte el autor mencionado, un tercero extraño pueda utilizar una IP si el titular no la aseguró debidamente con una contraseña, o la misma sea insegura, o incluso pueda ser utilizada por *hackers*, lo importante de destacar es que la dirección IP se constituye como un medio de prueba fundamental para el descubrimiento de los intervinientes en la mayoría de los ciberdelitos ya que, o bien puede directamente identificar a su autor, o bien hacerlo potencialmente identificable en tanto titular de un servicio de acceso a Internet.

c) Las herramientas con que cuenta la justicia

A fin de dar respuesta a las nuevas modalidades delictivas mediante la utilización de tecnologías, surgió hace algunos años la resolución 69/2016 del Ministerio de Justicia y de Derechos Humanos, que establece el denominado "Programa Nacional contra la Criminalidad Informática".

Mediante el mismo, se ha buscado proveer a la justicia penal de los elementos necesarios para la investigación eficiente de esta nueva forma de criminalidad compleja que resulta de los avances de las nuevas tecnologías, no solo para el caso de los delitos informáticos propiamente dichos, sino también para los casos de delitos tradicionales potenciados por las nuevas tecnologías, como el terrorismo, la trata de personas, el narcotráfico y lavado de activos, entre otros.

(10) Vaninetti, Hugo G.: "Delito de acceso ilegitimo a un sistema informático de acceso restringido" - LL - 2017 - pág. 460

(11) Cafferatta Nores, José I.: "La prueba en el proceso penal" - Ed. Depalma - Bs. As. - 1998 - pág. 193

Si bien resulta positiva toda mejora normativa que procure paliar la advertencia que planteaba Sueiro, lo cierto es que suele suceder que las burocracias se aferran a los métodos conocidos y ya utilizados, que parecerían no servir al fin propuesto en la resolución en análisis. Como podremos observar a través del punto V, las transformaciones que producen estas tecnologías de información y comunicación, explotadas por quienes delinquen mediante ellas, son mucho más rápidas que los procesos legislativos de creación y sanción de leyes, de modo que lo más probable es que, cuando el proyecto sea redactado y sancionado, ya resulte obsoleto en relación con el delito que buscaba castigar. A ello cabe sumar que una vez sancionada la normativa, corresponde la debida capacitación de los operadores, por lo cual, para que la misma sea efectivamente puesta en práctica puede transcurrir, al menos, un año. Finalmente, el programa mencionado nada dice en torno a la conservación de la evidencia digital, aspecto no menor, como pudimos observar antes, y que puede terminar siendo crucial en la investigación de muchos de estos casos.

V - ALGUNAS CONCLUSIONES

Tanto a partir del presente trabajo como de las jornadas preparatorias para el XIX Congreso Internacional de derecho penal "*Sociedad de la Información y Derecho Penal*[12]*",* presentamos una serie de conclusiones, a mi juicio edificantes, sobre el estado de la situación en lo atinente a la problemática probatoria en criminalidad informática.

1. Estado de la legislación procesal penal

Como se advirtió al comienzo del trabajo, una de las principales dificultades que presenta nuestro ordenamiento es que no se ha llevado a cabo una reforma procesal penal con respecto a la criminalidad informática. En tal sentido, la sanción de una ley que regule la obtención, almacenamiento y conservación de prueba digital deviene imprescindible, no solo para la unificación de criterios, sino para la viabilidad a largo plazo de las investigaciones aludidas.

La ley 26388 tuvo en consideración el Convenio sobre la Ciberdelincuencia de Budapest del 23/11/2001. Sin embargo, se limitó a seguir solo sus lineamientos parcialmente. Es decir, nuestra legislación nacional se adaptó únicamente respecto al derecho penal sustantivo, previsto en el Capítulo II -"Medidas que deberán adoptarse a nivel nacional"-, Sección 1 -"Derecho penal sustantivo"-. No adhirió nuestra legislación a la Sección 2 de este instrumento internacional, dedicada al derecho procesal. Por tal motivo, no se adoptaron medidas legislativas que permitan establecer procedimientos penales específicos para la obtención de prueba electrónica de cualquier delito cometido por medio de un sistema informático. Tampoco se dio 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.

(12) Informática y Delito. Reunión preparatoria del XIX Congreso Internacional de la Asociación Internacional de Derecho Penal AIDP - 1ª ed. - agosto/2014

2. Actuación policial

En lo atinente a la recolección de información, la actuación policial -basada en la inteligencia y los ciberpatrullajes que mencionábamos durante el trabajo- permite a las agencias de aplicación de la ley contar con elementos para la investigación y juzgamiento debidos. La principal técnica empleada es la geolocalización de equipos mediante la activación remota de GPS o del empleo de detección de antenas utilizadas por el dispositivo. En esta tarea aparece la detección de direcciones IP como elementos fundamentales para la determinación de la autoría en casos de cibercriminalidad.

La interceptación de telecomunicaciones móviles se encuentra prevista bajo el régimen general de los códigos procesales, ello mediante autorización judicial fundada. También existe el acceso a cuentas de correo electrónico, chat, o mensajería instantánea móvil. En particular, la mensajería instantánea móvil instalada en los celulares inteligentes (*smarthphones*), presenta serias dificultades para su posible investigación por parte de agencias judiciales y policiales debido a que este tipo de mensajería instantánea (BlackBerry Messenger, Whatsapp) se encuentra encriptada.

3. Conservación de evidencia digital

A la fecha, no existe una legislación nacional alineado con el Convenio sobre la Ciberdelincuencia de Budapest que prevea la conservación rápida de datos informáticos almacenados, la conservación y revelación parcial rápida de datos relativos al tráfico, su orden de presentación, su registro y confiscación, la obtención en tiempo real de datos relativos al tráfico y la interceptación de datos relativos al contenido.

En lo que tiene que ver específicamente con la cadena de conservación de la evidencia digital (recogida - almacenamiento - retención - producción - presentación - valoración de la prueba electrónica), pese a que se han realizado algunas modificaciones al Código Procesal Penal de la Nación, lo cierto es que por el momento no existe una reforma que permita contar con reglas específicas para la información relacionada con las TIC.

Es así que, ante la ausencia de una ley, no existen reglas de integridad o protocolos para la manipulación de prueba digital. Como se aclaró, en la Argentina rige el principio de libertad probatoria, de modo que no existen reglas sobre la admisibilidad, descubrimiento, revelación o valoración de las pruebas que son específicas de la información relacionada con las TIC.

Para dotar a las pruebas de las pautas de seguridad necesarias (no contaminación, no pérdida de las cadenas de seguridad, inalterabilidad) se recurre a peritos oficiales, como frente a cualquier otra prueba. En la etapa de juicio deben ser introducidas a pedido de parte y con el control de ellas como cualquier otra prueba.

4. Bases de datos públicas

Si bien por el momento no se pueden aplicar las técnicas de minería y comparación de datos para crear perfiles de posibles autores o grupos de riesgo -ya que no existen hasta la fecha organismos especializados en la construcción de información digital-, las agencias de aplicación de la ley tienen acceso a las bases de datos de la Administración Federal de Ingresos Públicos (AFIP), de la Administración de la Seguridad Social (ANSeS), de la Dirección General de Aduanas (DGA), de la Dirección Nacional de Migraciones (DNM) y del Banco Central de la República Argentina (BCRA), quienes suelen proveer elementos que muchas veces permiten la continuación de una pesquisa.

5. Información de empresas privadas

En lo que tiene que ver con el ámbito privado, si bien las empresas no se encuentran obligadas por ley a la conservación de información y datos, ante el requerimiento judicial suelen proporcionar información los proveedores de Internet (Speedy, Fibertel), los servidores de correos electrónicos (Hotmail, Yahoo, Gmail), los motores de búsqueda (Google, Yahoo) y las redes sociales (Facebook, Myspace, Hi5, Orkut, Sónico, etcétera).

De todos modos, es difícil obligar a dichas empresas de telecomunicaciones o proveedores de servicios a compartir los datos con las agencias de aplicación de la ley, ya que la mayoría de ellas son transnacionales. Por lo tanto, es difícil aplicarles medidas coercitivas o sanciones, además de que se rigen por sus políticas de privacidad para determinar en qué casos brindar información.

6. Tribunales y fiscalías especializadas

Si bien el Poder Judicial de la Nación, por medio de la CSJN, realizó profundas actualizaciones en materia de infraestructura tecnológica y capacitación del personal, en la actualidad no cuenta con tribunales especializados en materia de criminalidad informática o un área destinada específicamente a esta materia. En lo atinente al Ministerio Público Fiscal, se ha instaurado el rol de Fiscal en Cibercrimen en el marco de la Procuración General de la Nación, apoyado por la ya existente División Delitos Tecnológicos de la Policía Federal Argentina. Por su parte, el Ministerio Público de la Defensa, quien también posee una gran cantidad de comisiones y programas, como así también un importante Departamento de Informática dentro del área de la Dirección General de Administración de la Defensoría General de la Nación, hasta el presente no dispone de ninguna comisión o programa especializado en criminalidad informática.

7. Utilización de tecnologías en las investigaciones

La videovigilancia es una herramienta tecnológica permitida en espacios públicos, no así en espacios privados ni en domicilios, y se está utilizando cada vez con mayor frecuencia, no solo en lo atinente a la prevención delictiva sino en lo relativo a la investigación. Algunas leyes procesales penales provinciales regulan entre los medios de prueba a las filmaciones, aunque cabe aclarar que no se encuentra autorizada la escucha acústica de domicilio o el empleo de cámaras térmicas.

Por otra parte, se han implementado, sobre todo en el ámbito de la justicia federal, los métodos de declaración testimonial a distancia, así como de declaraciones indagatorias en los casos en que se dificulta en demasía la presencia del imputado ante los estrados del tribunal.

En la reconstrucción de los hechos se utilizan técnicas digitales y virtuales, como el empleo de mapas satelitales Google Maps, Google Earth, sistemas de coordenadas, GPS y programas y aplicaciones de geolocalización como *Foursquare*. Sí pueden utilizarse técnicas audiovisuales para presentar pruebas en el juicio (en su forma más simple: imágenes y sonido).

8. Implementación del expediente electrónico

A través de la ley 26685 se está realizando paulatinamente la transición al expediente digital y la gradual sustitución del expediente papel. Un significativo avance por parte del Poder Judicial de la Nación es la labor encarada por la Corte Suprema, que

ha digitalizado todas sus sentencias y gran parte de su biblioteca. En igual sentido, ha comenzado con los cursos de capacitación para la implementación gradual de la acordada 31/2011, tendiente a la constitución de domicilios electrónicos de notificación. No debe perderse de vista que, en un país con estructura federal, en el que los códigos procesales han quedado reservados a las provincias y, además, el Código Procesal Penal de la Nación es de los más antiguos -en cuanto a su adscripción a un sistema mixto con rasgos inquisitivos-, en el orden local puede haber previsiones más actuales, como las citadas de la Provincia de Buenos Aires, donde hoy es común que actos centrales del proceso se documenten mediante registración de audio/video digitales, con una breve acta escrita que complementa el legajo tradicional, dejándose constancia del acto celebrado.

Como se ha podido observar, resta mucho camino por transitar aún, pero quizás una de las claves sea la forma en que lo transitamos. Para que las respuestas a las modalidades de criminalidad informática tengan el efecto esperado deberemos dotarlas de similar mutabilidad, requiriéndose por parte de quienes tienen la tarea de brindar las herramientas legislativas y aquellos que tienen la misión de materializarlas en la realidad un abordaje distinto al tradicional. Quizás los primeros pasos que puedan darse sean extraíbles de algunas de las conclusiones que antes señalamos: avanzar en las debidas reformas procesales, utilizar protocolos que permitan a las fuerzas policiales una actividad más segura y uniforme en torno a la evidencia digital, capacitar tanto a estas últimas como a jueces, fiscales y defensores en las nuevas tecnologías, y finalmente gestar un fuero penal especial de criminalidad informática que pueda aprovechar debidamente todo ello.

Empleo de las direcciones virtuales como elemento fundante en las declaraciones de incompetencia por territorialidad

María E. Darahuge(*)
Luis Arellano González(**)

I - EXORDIO

Considerando que la jurisdicción es el poder del Estado de juzgar o de ejercer la función judicial, la competencia es la medida en que ese poder del Estado le es dado a un tribunal determinado. La competencia(1) delimita la zona de conocimiento, intervención, decisión y ejecución del juez o tribunal, determinando el espacio, materia y grado de los asuntos que le incumben. La competencia es improrrogable por simple voluntad de los sujetos de un procedimiento. Además, es inalterable, ya que el único parámetro para atribuir competencia a un tribunal es la ley y, por lo tanto, deviene en absoluta.

De ahí que sea sumamente importante establecer con claridad y precisión reglas que permitan deslindar la misma en los casos en los que ocurre oposición a recibirla o reclamo para ejercerla por parte de un determinado tribunal ("aceptación de competencia o declaración de incompetencia" normalmente sometida al arbitrio del respectivo superior).

(*) Licenciada e ingeniera en Informática (UCASAL). Máster en Dirección Estratégica en Tecnología de la Información (Universidad Europea del Atlántico, España). Especialista en Criptografía y Seguridad Teleinformática (Universidad de la Defensa). Doctora en Psicología Social (Universidad Kennedy). Coautora de los Manuales de Informática Forense I, II y III (ERREPAR). Perito judicial
(**) Abogado con orientación penal (UBA). Ingeniero en Informática (UCASAL). Licenciado en Criminalística (IUPFA). Licenciado en Informática (UCASAL). Especialista en Criptografía y Seguridad Teleinformática (Universidad de la Defensa). Perito en Documentología, Balística y Papiloscopía (IUPFA). Coautor de los Manuales de Informática Forense I, II y III (ERREPAR). Perito judicial

(1) Dentro de la República Argentina, como consecuencia directa del sistema federal de gobierno, existe la competencia ordinaria, normal o habitual. Esta es una facultad no delegada de las provincias a la Nación, mientras que la federal es excepcional, limitada y circunscripta a determinado ámbito territorial, personas y cosas en relación con el Estado Nacional y a algunas materias específicas

En nuestro caso, nos abocaremos al problema de determinar dicho espacio de competencia, en relación con el área geográfico-política donde ocurrió un determinado evento susceptible de judicialización.

Por el contrario, no pretendemos decidir sobre las múltiples cuestiones que facultan o sustentan a un tribunal en su declaración de incompetencia, sino aportar un elemento de decisión más a dicha cuestión y su posterior aprobación o desestimación por parte del superior que resuelve el incidente cursado. Este elemento es la ubicación, cierta, precisa y delimitada de un evento físico en cuanto a su ocurrencia espacial y geográfica a partir de los datos resguardados como resultado de un evento digital asociado al tema a dilucidar.

II - INTRODUCCIÓN

Conceptos destacables a considerar

- La competencia provincial es la regla y se ocupa del juzgamiento de los delitos comunes y contravenciones o faltas dentro de cada provincia.
- La territorialidad es la nota característica de la competencia. Es decir, los jueces, por regla, son competentes para resolver todas las causas suscitadas en el territorio que la ley les asigna para el ejercicio de su jurisdicción.
- La primera regla es que el juez competente es el del lugar de comisión del delito, su base dogmática se encuentra en el artículo 118 de la CN. Para llevar a la práctica esta regla, cada provincia, al dictar las leyes orgánicas del Poder Judicial, ha dividido sus territorios dentro de cuyos límites se atribuye la competencia penal a un juez o grupo de jueces entre los cuales se reparte, a su vez, el conocimiento de las causas. Sobre la base de esta distribución no debe [o no debería[2]] quedar ningún espacio del territorio sin juez.
- La finalidad se funda en la proximidad del tribunal al lugar del hecho para favorecer la garantía de defensa en juicio y el principio de economía procesal, pues favorece la rápida, sencilla y más económica investigación.
- Aunque el problema de la competencia afecta transversalmente a la totalidad de la jurisdicción y los distintos fueros del derecho argentino, pondremos énfasis en el derecho procesal penal, ya que las nuevas modalidades delictivas soportadas en medios digitales (narcotráfico, trata de personas, pornografía infantil, terrorismo, entre otros) agregan un nuevo componente de incertidumbre a dicha problemática.[3]

(2) Este potencial se relaciona con ciertos problemas que, aunque integran el derecho internacional público, no están absolutamente definidos y delimitados, por ejemplo, la franja limítrofe cordillerana, en la frontera con nuestro vecino país Chile y algunas otras excepciones que trascienden y escapan del análisis de este artículo

(3) CPPN. **Art. 34** - "*Para determinar la competencia se tendrá en cuenta la pena establecida por la ley para el delito consumado y las circunstancias agravantes de calificación, no así la acumulación de penas por concurso de delitos de la misma competencia. Cuando la ley reprima el delito con varias clases de pena, se tendrá en cuenta la cualitativamente más grave*".

Art. 35 - "*La incompetencia por razón de la materia deberá ser declarada aun de oficio en cualquier estado del proceso. El tribunal que la declare remitirá las actuaciones al que considere competente, poniendo a su disposición los detenidos que hubiere.*

- El momento de la comisión de un delito: en principio, un delito penal se considerará cometido en el lugar de su consumación definitiva, cuando ya se realizaron todos los actos previstos por la ley como constitutivos del delito. Pero no todos los casos se presentan de manera sencilla. Si el delito ha sido tentado, en ese caso, será competente el juez del lugar donde se cumplió el último acto de ejecución. Si se tratara de un delito continuado (varias acciones típicas autónomas que se consideran como un solo delito, como una sola acción típica que se prolonga en el tiempo), será competente el juez del lugar donde cesó de cometerse. Finalmente, si se ignora o duda en qué lugar se cometió el delito, será competente el juez que primero haya prevenido.
- En cualquier estado del proceso, el tribunal que reconozca su incompetencia territorial deberá remitir la causa al competente, poniendo a disposición a los detenidos, si los hubiere. Sin perjuicio de realizar los actos urgentes de la investigación. La declaración de incompetencia territorial no produce la nulidad de actos cumplidos.
- Otras formas de competencia: por la materia, por conexidad, por acumulación de procesos.
- Cuestiones de competencia: son aquellas que surgen cuando dos órganos jurisdiccionales se declaran en forma simultánea y contradictoria competentes o incompetentes para la investigación o juzgamiento de un mismo hecho. Asimismo, se presenta de modo positivo cuando dos o más jueces pretenden conocer del mismo hecho, y de manera negativa, cuando rehúsan su intervención. El conflicto surge tanto cuando el juez decide oficiosamente sobre su competencia o cuando ello es planteado por las partes.
- Inhibitoria, declinatoria: el trámite para resolver estos conflictos se concreta mediante la "inhibitoria" o "declinatoria". Si ante los referidos planteos los jueces no aceptan lo pertinente, corresponde la decisión a quien resulte superior jerárquico común de los enfrentados.
- Las cuestiones de competencia no suspenderán la investigación que será continuada por el juez que primero haya conocido en la causa. Este punto es muy importante en el tema que vamos a analizar, ya que la celeridad y la confidencialidad en los actos preliminares a la constitución de prueba documental informática son de tal pertinencia que su retraso puede derivar en la pérdida o nulidad de los elementos probatorios necesarios para delimitar físicamente el evento y decidir sobre la competencia en

Sin embargo, fijada la audiencia para el debate sin que se haya planteado la excepción, el tribunal juzgará los delitos de competencia inferior".

Art. 36 - "*La inobservancia de las reglas para determinar la competencia por razón de la materia producirá la nulidad de los actos, excepto los que no pueden ser repetidos, y salvo el caso de que un tribunal de competencia superior haya actuado en una causa atribuida a otro de competencia inferior".*

Art. 37 - "*Será competente el tribunal de la circunscripción judicial donde se ha cometido el delito. En caso de delito continuado o permanente, lo será el de la circunscripción judicial en que cesó la continuación o la permanencia.*

En caso de tentativa, lo será el de la circunscripción judicial donde se cumplió el último acto de ejecución".

Art. 38 - "*Si se ignora o duda en qué circunscripción se cometió el delito, será competente el tribunal que prevenga en la causa".*

Art. 39 - "*En cualquier estado del proceso, el tribunal que reconozca su incompetencia territorial deberá remitir la causa al competente, poniendo a su disposición los detenidos que hubiere, sin perjuicio de realizar los actos urgentes de instrucción".*

Art. 40 - "*La declaración de incompetencia territorial no producirá la nulidad de los actos de instrucción ya cumplidos"*

ciernes. Al respecto, todos los actos practicados hasta la definición del tribunal competente serán válidos, aunque el tribunal a quien corresponda definitivamente el proceso podrá ordenar su ratificación y/o ampliación.

La problemática tecnológica

Considerando que la evolución de la tecnología nos ha llevado a escindir el conocido "lugar del hecho", en sus nuevas versiones: lugar del hecho real (LHR), lugar del hecho virtual impropio (LHVI) y lugar del hecho virtual propio (LHVP), deviene necesario analizar cada una de las situaciones que estos novedosos escenarios implican para establecer la ubicación cierta de un componente digital determinado o determinable.

Lugar del hecho real (LHR)

El lugar del hecho real es el área definida y determinada en espacio y tiempo donde ocurre un evento o una serie de ellos. Los operadores del derecho están familiarizados con el mismo y acostumbrados a gestionarlo con solvencia judicial (en particular, procesal meridiana). Múltiples teorías respecto de la competencia a partir de la ubicación geográfica del mismo han obtenido una serie muy extensa de resultados jurisprudenciales que avalan la resolución de un problema de competencia basado en el territorio. No es motivo de este trabajo analizar sus pormenores e implicancias jurídicas. Sin embargo, es imprescindible considerar:

- Toda información es información codificada (en cualquier lenguaje que pueda ser concebido e implementado: castellano, binario, ruso, cobol, latín, hexadecimal, etc.). En tanto y en cuanto la información pueda ser representada (recordemos que si algo no puede ser representado, entonces simplemente no existe, al menos para la ciencia), entonces podrá ser codificada y almacenada en algún soporte físico.(4)
- Esta información codificada está en uno de tres estados: almacenada, en tránsito o en transformación, pero siempre ocupa un lugar en el espacio y es contenida por elementos materiales, de existencia real (los electrones o los fotones son partículas y no fantasmas, nos guste o no).
- En tal sentido, siempre es posible establecer dónde se encuentra determinada información en un momento dado. A veces, el tiempo de permanencia en el lugar es casi efímero, pero nunca es nulo. El caso más crítico es aquel en el que la información está siendo transformada en el núcleo de una computadora (ALU, registros, buses de datos y direcciones y otras circunstancias similares), lo que agrega complejidad a la determinación de la posición exacta de la información, pero no la sustrae al espacio tiempo en que discurrimos nuestras terrenales existencias.
- Como colofón, podemos afirmar que siempre existe un lugar del hecho real, ya sea que esté restringido a un área determinada o que se encuentra distribuido en varias áreas geográficas, relacionadas por eventos informáticos en desarrollo. Aunque pueden existir múltiples copias idénticas de un archivo digital, eso no implica que un mismo archivo pueda existir en dos dimensiones al mismo tiempo.

(4) A pesar de la resistencia que puede generar esta afirmación, no tenemos constancia alguna que lugares como: el Vahala, el Nirvana, el Paraíso, la dimensión crepuscular (léase dimensión desconocida, al sur del Trópico de Cáncer) y el ciberespacio tengan existencia real mensurable por medios físicos corrientes (en contra de la opinión de los jugadores de WOW, comunidad a la pertenecen ambos autores)

- Introyectar, asimilar y adoptar como propio el concepto anterior resulta imprescindible para el operador del derecho del siglo XXI. Pretender que existe un "ciberespacio", desprendido de la realidad y solo accesible a los jóvenes que integran la cultura "digital", es la principal causa de los errores en la gestión de la prueba documental informática que a diario debemos sufrir los justiciados y/o justiciables, violentando profundamente el orden y la seguridad jurídica en que la mayoría de los mortales pretendemos convivir. La solución no reside en la edad del analista, sino en su capacidad de adaptarse a la evolución tecnológica que lo rodea, a su interés por capacitarse y sobre todo a la necesidad de abandonar la creencia soberbia y reemplazarla por la crítica lógica y constructiva (a pesar de lo que pretendan las teorías en boga, los vocablos "sano" y "crítica" pocas veces se pueden compatibilizar entre sí, en particular porque ambos son ambiguos, relativos y multívocos).

Lugar del hecho virtual impropio

Cuando el lugar del hecho real es relevado, registrado y almacenado por medios digitales, en una simulación estática o dinámica, con la fidelidad, detalle y definición que la tecnología moderna permite, estamos ante un lugar del hecho virtual impropio. Se lo denomina impropio porque existe una correspondencia biunívoca entre el lugar del hecho real y su representación digital (estática o dinámica). De esta forma se pueden hacer reconstrucciones de hechos para determinar si los resultados obtenidos se corresponden con la evidencia registrada en el lugar del hecho real. Pensemos, por ejemplo, en la dinámica del movimiento vehicular, que se desarrolla en el marco de una pericia de accidentología vial y la posibilidad de repetir las veces necesarias el experimento, modificando las condiciones iniciales, hasta que la correspondencia con lo comprobado en el lugar del hecho real sea lo más perfecta y ajustada posible. Tiene múltiples ventajas, por ejemplo, la comparación entre expertos locales o remotos, el resguardo del lugar a pesar del paso del tiempo (correctamente resguardado, certificado y con su correspondiente cadena de custodia), evitar la coordinación de agendas entre profesionales hiperespecializados y con escaso tiempo disponible, encuentros que pueden ser reemplazados por videoconferencias, con resultados similares a los obtenidos mediante la inspección o el reconocimiento judiciales clásicos. En este caso, no existen problemas de competencia, ya que la misma está determinada específicamente por el lugar del hecho real, del cual el lugar del hecho virtual impropio es solo una reconstrucción.

Lugar del hecho virtual propio

En este caso, las acciones ocurren completamente en entornos virtuales. Por ejemplo, un falsario desde Buenos Aires utiliza, por medios remotos, una granja de servidores en Medio Oriente, para descubrir una clave de acceso a una cuenta bancaria en Holanda y transferir fondos desde Barcelona a Punta del Este, con el objeto de cobrar el dinero en una sucursal de Piriápolis. La única forma de representar estas transacciones es por medio de una simulación virtual, no existe la correspondencia con un LHR.

En este caso, no es posible emular y solo queda la solución de la simulación, es imposible escapar a la subjetividad de quien propone e implementa dicha simulación; en realidad, la labor pericial se diluye y solo resta la tarea testimonial del experto. Solo se puede contrastar mediante el empleo de un colegio de peritos, con asistencia del juez, en reemplazo del clásico careo testimonial. Es decir, el colegio de peritos es al careo lo que el testigo experto al testigo.

La única figura que se puede utilizar es el reconocimiento/inspección judicial virtual, local o remota, no se encuentra específicamente descripto, ni detallado en la codificación procesal vigente en nuestro país. Por lo tanto, los temas relacionados con delitos informáticos propios, como ser la sustitución de identidad virtual, suelen ser muy difíciles de probar, ya que la prueba no se puede encuadrar en las figuras procesales vigentes.

Al igual que la obtención (legítima o ilegítima) de prueba confesional y/o testimonial, utilizando mecanismos de análisis de contenido neuronal (memoria) por métodos no invasivos, sustentados por neurociencias, constituyen una auténtica laguna procesal por el momento.(5)

Este es el punto álgido de la cuestión. Ahora, el problema de la competencia se vuelve crítico, ya que podría ocurrir que existan elementos probatorios del delito en distintos lugares del mundo y la comisión del mismo no siempre está perfectamente definida. Las situaciones posibles pueden devenir en:

1. Suponiendo establecida la competencia de un tribunal nacional:
   a) Elementos probatorios obrantes en un país con el cual existen convenios bilaterales de asistencia judicial/policial recíproca. El caso más sencillo es Argentina-Uruguay.
   b) Elementos probatorios obrantes de un país con el cual existen tratados multilaterales de similar índole (por ejemplo, Paraguay-Argentina y su inserción en el Mercosur o Argentina y otro país que integre la OMC o la UIT). Se comienza a complicar porque estos convenios normalmente son mucho más limitados que los anteriores.
   c) Elementos probatorios obrantes en un país con el cual no existen vínculos de asistencia judicial/policial de ningún tipo, por ejemplo, Iraq o Irán. El peor de los casos implica que no va a ser posible obtener dato alguno por medios judiciales lícitos. El ejemplo típico es el uso de granjas de servidores situados en Medio Oriente (por ejemplo, Siria) para romper claves bancarias.
2. Suponiendo la indeterminación o duda sobre la competencia de un determinado tribunal, ya sea que se excusen o sean recusados. El problema es de difícil solución.

Aporte de la informática y la informática forense en la resolución del problema

Explicación técnica informática

Cada dispositivo informático fijo o móvil está asociado mediante su placa de red/comunicaciones con una dirección física única que identifica a dicha placa. Es decir, es un número hexadecimal, normalmente denominado dirección MAC, que es propio del

(5) La sustitución del viejo y obsoleto polígrafo, como detector de mentiras, por los nuevos escáneres magnéticos no invasivos, constituye uno de los ejemplos vigentes y en uso diario por aquellas instituciones que disponen de dicha tecnología (entre otros, la NSA, la CIA y el FBI). Hasta la fecha (mayo/2018), el tema sigue en disputa entre aquellos que sostienen la prioridad del derecho de la sociedad a defenderse, por sobre el derecho a la privacidad y aquellos que lo ven como una especie de autoinculpación involuntaria e inevitable, que iría contra el derecho a no declarar contra sí mismo. El tema está abierto en el mundo y al parecer es cuasi desconocido por nuestra sociedad en general y nuestros operadores del derecho (funcionarios o no) en particular. El derecho siempre corre tras la tecnología, pero al parecer, la segunda le está sacando demasiada ventaja, lo que obra contra la necesidad social de seguridad jurídica que nos incluye a todos

dispositivo y único respecto de los demás. Luego, cada usuario que utiliza el dispositivo se identifica con el mismo de manera biunívoca mediante una dirección IP.

Ahora bien, como dijimos, la información siempre se encuentra en algún lugar fijo, más aún en un dispositivo determinado. Por lo tanto, si determinamos la dirección IP de origen o destino (según el caso de que se trate) de una transacción digital, habremos establecido el lugar de ocurrencia de un evento virtual, que puede resolvernos de manera unívoca el problema de la competencia judicial.

Es cierto que si la dirección IP está asociada a un dispositivo móvil, el problema se traslada a establecer con precisión dónde se encontraba dicho dispositivo al momento en que ocurrió el evento investigado. Este problema no es un problema informático y deberá ser considerado por otras pruebas complementarias, como testimonios, geolocalización, pruebas de informes, reconocimiento/inspección judicial y cualquier otro que contribuya a reducir la incertidumbre acerca de la localización del dispositivo en un momento dado. Por supuesto, este método no soluciona la problemática general de la competencia, ya que dependerá del criterio que utiliza quien analiza y determina la misma (el lugar de ocurrencia, el lugar donde se lo ejecutó, la nacionalidad del delincuente). Insistimos, no solucionamos los problemas teóricos y prácticos que la determinación de competencia en lugares de hecho reales ha provocado a lo largo de los siglos. Sin embargo, sí permite establecer con claridad en qué lugar lógico ocurrió un evento y dónde se encontraba el dispositivo que generó el evento en el momento en que dicho evento se produjo.

III - SINTETIZANDO

En el caso de resolver problemas de competencia relacionados con lugares del hecho virtuales propios (LHVP), la determinación de la dirección IP de cada dispositivo/usuario comprometido en el mismo permite esclarecer su lugar de ubicación. No soluciona los problemas de fondo de la competencia, los cuales siguen siendo los que históricamente se han relacionado con el lugar del hecho real (LHR), aunque permite dilucidar ubicaciones y localizaciones que facilitan dicha determinación.

IV - COLOFÓN

En aquellos casos en los que la determinación de la competencia requiera establecer la ubicación político-geográfica de un determinado usuario/dispositivo correspondiente al origen o destino de un evento digital, el magistrado decisor debería solicitar un informe técnico que determine la dirección IP del referido dispositivo, su dirección MAC asociada y su geolocalización al momento del evento considerado. Procesalmente, la medida debería ser incluida en autos como medida previa, preliminar o prueba anticipada, según el fuero y derecho procesal codificado que corresponda. El resultado de este informe brindaría sustento objetivo al argumento de declinación o aceptación de la competencia cuestionada legalmente.

ERREIUS

Paraná 725, CABA (1017), Buenos Aires | Argentina
(011) 4370-2018
contactenos@erreius.com

www.erreius.com