El convenio de Budapest y su influencia en el derecho penal argentino

Facundo E. Hertler[1]

SUMARIO: I.- Informática y delito. Necesidad de límites; II.- El "Convenio de Budapest" como primera manifestación internacional en la lucha contra el cibercrimen, III.- Recepción del convenio en la Argentina mediante ley 26.388: delitos comprendidos; IV.- Las significaciones incorporadas al art. 77 del C.P; V.- Acceso ilícito; VI. - Interceptación ilícita; VII.- Ataques a la integridad de los datos y del sistema; VIII.- Abuso de los dispositivos; IX.- Falsificación informática; X.- Estafa informática; XI.- Pornografía infantil; XII.- Propiedad intelectual; XIII.- Conclusiones; XIV.- Bibliografía

RESUMEN: El presente artículo analiza el avance legislativo a nivel nacional y convencional en materia de ciberdelincuencia. Concretamente se toma al Convenio de Budapest como normativa de referencia, un documento internacional que en el año 2021 cumplió dos décadas desde su firma. La normativa internacional mencionada ha influenciado a la Argentina en la creación de su ley de delitos informáticos (ley 26.388), habilitando así la punición de la ciberdelincuencia a nivel local. Respecto de esta normativa nacional, se hará en este artículo un reducido análisis dogmático, a fin de comprender sus características principales, tanto desde una perspectiva sistemática como comparativa, determinando las diferencias y

[1]Abogado (UNNE - Corrientes, Argentina). Magister en Ciencias Penales (UNNE - Corrientes, Argentina). Profesor Adjunto del curso de Derecho Penal General (UCP - Presidencia Roque Sáenz Peña, Argentina). Secretario de Primera Instancia y Defensor Público Coadyuvante en la Defensoría Pública Oficial ante el Juzgado Federal de Presidencia Roque Sáenz Peña - Ministerio Público de la Defensa (MPD - Argentina). Correo electrónico: facundohertler@gmail.com

similitudes entre aquella y el Convenio de Budapest. A modo de conclusión, se hará una breve mención respecto de la competencia para la investigación de estos hechos y las conductas que se encuentran pendientes de recepción por la ley penal.

PALABRAS CLAVE: Convenio – internacional – ciberdelitos – Argentina - ley penal

ABSTRACT: This article analyzes the legislative progress at the national and conventional levels in terms of cybercrime. Specifically, the Budapest convention, an international document that has been signed two decades ago, is taken as a reference body of law. This Convention has influenced the creation of the Argentine law of cybercrime (Act No 26.388); thus, punishment of cybercrime was enabled at the local level. Regarding this national rule, in this article a brief dogmatic analysis is performed with the aim of understanding its main characteristics, from both a systematic and comparative perspective; the differences and similarities between the Argentine Act and the Budapest convention are determined. To conclude, jurisdiction for the investigation of these crimes and the behaviors that are still pending of being provided by the criminal law are mentioned.

KEY WORDS: Convention – internacional – cybercrimes – Argentina - criminal law

I.- Informática y delito. Necesidad de límites

Con las nuevas tecnologías que nacen a partir de las exigencias propias de un mundo globalizado, se establece un nuevo paradigma, caracterizado por una democratización radical de la información y del acceso a vías de comunicación. Hoy en día se puede ser parte en una conversación por videoconferencia de un punto del globo a otro mediante un dispositivo de bolsillo, o compartir videos, fotos y documentos de manera instantánea, algo que en el siglo pasado era totalmente inimaginable. Sin embargo, no todas son virtudes y bondades en esta revolución informática, pues también en su seno se han manifestado nuevas formas de afectación a los bienes jurídicos, como así también nuevos bienes jurídicos objetos de protección.

Por ello, debido a los riesgos que encuentra la sociedad posmoderna[2] en favor de una mejor calidad de vida (en este caso particular respecto de la comunicación y la información), surge la necesidad de que el Estado, en ejercicio de su *ius puniendi*, limite el empleo desmedido de las TIC[3] por sus usuarios cuando estas produzcan un perjuicio a terceros. Esta práctica implica actos que van desde la captación ilegal de datos o comunicaciones electrónicas, mediante infiltraciones en diversos dispositivos (móviles, computadoras, servidores, etc.), o en bancos de información en organismos públicos o privados, hasta diferentes formas de afectación a la integridad sexual: producción y distribución de pornografía infantil en la web, la existencia de redes de pedofilia, y muchos otros hechos que escapan a la imaginación. Las prácticas de hacking[4] y cracking, la utilización de malware[5], troyanos, bombas lógicas, gusanos, ransomware[6] y el sinnúmero de virus[7] creados a la fecha, son solo algunas herramientas utilizadas por usuarios malintencionados para obtener sus propósitos.

En función de las circunstancias expuestas, los países del mundo han manifestado su preocupación por limitar (sino erradicar) el cibercrimen, a través de la creación de nuevos tipos penales para la persecución concreta de esos hechos. Sin embargo, a mayor tiempo que pasa, se generan nuevas formas de lesión a los bienes jurídicos por este medio, dejando a la legislación siempre a un paso atrás.

II.- El "Convenio de Budapest" como primera manifestación internacional en la lucha contra el cibercrimen

Debido a las serias lesiones a los bienes jurídicos cometidas mediante las TIC, el 23 de noviembre 2001 el Consejo de Europa se reunió en Budapest, Hungría, para

[2] Rubio, J. H. (2019). Internet y postmodernidad: un soporte de comunicación tan necesario como irreverente en la actualidad. Necesidades pedagógicas. Vivat Academia, (146), 21-41. https://doi.org/10.15178/va.2019.146.21-41.

[3] TICs (05 de agosto de 2021). Etecé. Recuperado de: https://concepto.de/tics/

[4] Lucena Herrera C. (19 de agosto de 2019). Qué es el hacking. OpenWebinars. Recuperado de: https://openwebinars.net/blog/que-es-el-hacking/

[5] Bodnar C. (29 de octubre de 2013) Clasificación de Malwares. Kaspersky daily. Recuperado de: https://latam.kaspersky.com/blog/clasificacion-de-malwares/1608/

[6] A una semana del ciberataque del Ransomware Wannacry, siguen los esfuerzos para frenarlo (19 de mayo de 2017). Télam. Recuperado de en: http://www.telam.com.ar/notas/201705/189655-ciberataqueransomware-wannacry.html

[7] Galindo Domínguez Y. (26 de septiembre de 2005) ¿Qué son los virus informáticos?. Desarrolloweb.com. Recuperado de: https://desarrolloweb.com/articulos/2176.php

firmar el Convenio sobre Ciberdelincuencia[8], siendo el primer tratado internacional que trata la cuestión, estableciendo tipos penales específicos, herramientas determinadas de investigación y de obtención de prueba, y, además, reglas relativas a extradición y asistencia internacional entre los países signatarios. La bondad de este tratado es que permite la incorporación de países no europeos a sus cláusulas, llegando a obtener un total de 54 ratificaciones y adhesiones[9].

El convenio aborda las normas de derecho penal sustantivo[10] en el Capítulo II, Sección I, agrupando las mismas en tres diferentes títulos. El Título I enumera los "Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos", tipificando el acceso ilícito, la interceptación ilícita, los ataques a la integridad de datos, los ataques a la integridad del sistema, y el abuso de dispositivos (arts. 2 y 3, 4, 5, 6 CB[11]). Luego, en el Título II, el instrumento internacional consagra los "Delitos informáticos" abarcando a la falsificación informática y al fraude informático (arts. 7 y 8 CB).

Continúa con los llamados "Delitos relacionados con el contenido" (Título III), comprendiendo los delitos implicados con la pornografía infantil (art. 9 CB), condenando la producción con fin de difusión (inc. 1.a), la oferta o puesta a disposición (inc. 1.b), la difusión o transmisión (inc. 1.c), adquisición (inc. 1.d), y posesión (inc. 1.e) de pornografía infantil en sistemas informáticos.

En el Título IV, se expresan los "Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines", desarrollando esta especie de delitos en un apartado del mismo nombre (art. 10 CB), haciendo alusión a la protección de los derechos de autor, en contra de la piratería en la web.

[8] Council of Europe. Convenio sobre la ciberdelincuencia (ETS No. 185). Budapest, 23.XI.2001. Recuperado de https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa41c

[9] Ratificaciones y adhesiones del Convenio de Budapest al 03 de octubre de 2021. Recuperado de: http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=TomHTOvO

[10] En el presente trabajo, únicamente se analizarán los delitos creados por el CB, es por ello que se ha omitido la mención a las cuestiones procesales y sobre cooperación internacional que el tratado prevé.

[11] A los fines prácticos, se designará con las siglas CB al Convenio de Budapest sobre Ciberdelincuencia.

Luego de ello (dentro del mismo título), se establecen ciertas disposiciones comunes para todos los delitos de la Sección I, vinculadas a la tentativa y la complicidad (art. 11 CB), a la responsabilidad de las personas jurídicas (art. 12 CB), y, por último, a las sanciones y medidas aplicables (art. 13 CB), debiéndose aclarar en este punto que el convenio no determina penas específicas. Sin embargo, se enuncian ciertos principios limitadores al *ius puniendi* para los Estados Parte en la consagración local de estos delitos, debiendo ser sus sanciones efectivas, proporcionadas y disuasorias, tanto en las penas privativas de libertad para las personas físicas, como en las pecuniarias para las jurídicas.

III.- Recepción del convenio en la Argentina mediante ley 26.388: delitos comprendidos

La aprobación local del Convenio de Budapest, de reciente data en nuestro país mediante ley 27.411 del 22 de noviembre de 2017[12], ha reafirmado la política criminal de Argentina en cuanto a la punición de la criminalidad informática, tendencia que se ha manifestado desde 2008[13]. Sin embargo, dicha aprobación legislativa está sujeta a reservas basadas en la normativa local vigente, las cuales abordaremos en los puntos siguientes. La punición concreta de estos hechos surge de la ley 26.388 de delitos informáticos, cuyo análisis dogmático lo plantearemos a continuación.

IV.- Las significaciones incorporadas al art. 77 del C.P

Previo a ingresar al análisis de las modificaciones e incorporaciones delictivas que nos ofrece la ley de delitos informáticos, cabe hacer mención de los términos ingresados al art. 77 CP. La ley 26.388 en su artículo 1º incorpora el concepto de documento, adoptando un carácter más amplio con relación a la anterior redacción. Así, la normativa establece que documento es *"toda representación de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión"*. Al declararse la "independencia del soporte", éste no sólo incluiría al papel, sino también a toda información contenida en un sistema de almacenamiento electrónico como discos rígidos o SSD (extraíbles o permanentes), servidores en la nube, etc. Además, las previsiones del art. 78 bis son trasladadas al art. 77 para comprender el

[12] Ley 27.411. Recuperada de: InfoLEG - Ministerio de Justicia y Derechos Humanos - Argentina

[13] En los considerandos de la Res. Conjunta N° 866/2011 y 1500/2011 -que crea la Comisión Técnica Asesora de Cibercrimen-, se advierte el compromiso de la nación Argentina respecto al cibercrimen en el plano internacional. Recuperado de: http://servicios.infoleg.gob.ar/infolegInternet/anexos/185000- 189999/188231/texact.htm.

núcleo de conceptos que ofrece la ley penal, estableciendo que los términos "firma" y "suscripción" abarcan *"la firma digital, la creación de una firma digital o firmar digitalmente"*. También se modifican los alcances del concepto de instrumento privado y certificado, comprendiendo en dichos términos al *"documento digital firmado digitalmente"*. Estas modificaciones permiten la adecuación de la normativa local a las previsiones del art. 7 del CB (referidas a la falsedad informática), ampliando así el alcance de los delitos contra la fe pública en dirección al ámbito digital, actualizando la protección de bienes jurídicos mediante el establecimiento de nuevos objetos de protección.

Es importante agregar que el CB también posee una serie de definiciones en su Capítulo I llamado "terminología", que hoy son vinculantes y complementarios a nuestra legislación penal, por efecto de la sanción de la ley 27.411. Así la norma internacional expresa en su art. 1º las definiciones de *"sistema informático"*, *"datos informáticos"*, *"proveedor de servicios"* y *"datos relativos al tráfico"*. Los mismos se transcriben a continuación:

"…A los efectos del presente Convenio:

a) Por «sistema informático» se entenderá todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, siempre que uno o varios de ellos permitan el tratamiento automatizado de datos en ejecución de un programa;

b) por «datos informáticos» se entenderá cualquier representación de hechos, información o conceptos de una forma que permita el tratamiento informático, incluido un programa diseñado para que un sistema informático ejecute una función;

c) por «proveedor de servicios» se entenderá:

i) Toda entidad pública o privada que ofrezca a los usuarios de sus servicios la posibilidad de comunicar por medio de un sistema informático, y

ii) cualquier otra entidad que procese o almacene datos informáticos para dicho servicio de comunicación o para los usuarios de ese servicio;

d) por «datos sobre el tráfico» se entenderá cualesquiera datos informáticos relativos a una comunicación por medio de un sistema informático, generados por un sistema informático como elemento de la cadena de comunicación, que indiquen el origen, destino, ruta, hora, fecha, tamaño y duración de la comunicación o el tipo de servicio subyacente…".

Habiendo expresado los conceptos otorgados por la ley penal local (mediante las incorporaciones al CP por la ley 26.388), y por el instrumento internacional (que se suman a nuestra legislación local mediante ley 27.411), corresponde a continuación abordar los delitos que ambos instrumentos consagran.

V.- Acceso ilícito

La ley 26.388, artículo 3º, modifica la denominación del Capítulo III ubicado en el Libro II, Título V del CP, por el de "Violación de Secretos y de la Privacidad", sustituyendo una serie de tipos penales para abarcar toda forma de intrusión a componentes electrónicos de manera ilícita y/o interceptación de comunicaciones (email, streaming, etc.). El capítulo también abarca normas que sancionan conductas pasibles de dañar y/o modificar información tanto privada como pública de acceso restringido, bloquear sistemas o bancos de datos, etc.

En cuanto al acceso ilícito, este fue incorporado al código penal mediante el art. 153 bis, el cual establece que: *"…Será reprimido con prisión de quince (15) días a seis (6) 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 (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…".*

Así también, se incorpora el art. 157 bis del CP, inc. 1, el cual prevé en su parte pertinente:

"…Será reprimido con la pena de prisión de un (1) mes a dos (2) 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…".

Estas previsiones buscan dar respuesta al CB en la punición del hacking intrusivo, el cual figura en el art. 2 del referido instrumento internacional:

"…Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno el acceso deliberado e ilegítimo a la totalidad o a una parte de un sistema informático. Cualquier Parte podrá exigir que el delito se cometa infringiendo medidas de seguridad, con la intención de obtener datos informáticos o con otra intención delictiva, o en relación con un sistema informático que esté conectado a otro sistema informático…".

El bien jurídico que busca proteger la ley penal es la privacidad del individuo (153 bis CP) o de un banco de datos (157 bis, inc. 1, CP) y los secretos que en su esfera privada se albergan.

La acción típica en ambas previsiones legales consiste en acceder a un sistema informático sin la debida autorización o excediéndose de ella, es decir, ingresar a determinados espacios donde solo el propietario del sistema o un tercero con su venia podrían y en el alcance que el último ofrece. El hacker accede por diversos mecanismos o programas, para captar o descifrar las claves posibles para el ingreso a cuentas en la web. Estos mecanismos pueden involucrar desde el empleo de técnicas de ingeniería social mediante "phishing"[14], "SIM Swapping"[15], hasta el uso de malwares que ingresan a los sistemas mediante descargas de software, de archivos, etc.

Se establece un agravante en el art. 153 bis CP, cuando el acceso sea a un sistema o dato perteneciente a *"…un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros…"*.

En cuanto al tipo subjetivo, los elementos *"a sabiendas"* (153 bis) e *"ilegítimamente"* (157 bis, inc. 1) refuerzan la idea de que es un delito doloso, que exige dolo directo.

Respecto de la autoría, el hecho puede ser cometido por cualquier persona. Respecto de la caracterización de estos hechos, los descritos en el art. 153 bis y 157 bis, inc. 1, pertenecen a la categoría de los delitos de pura actividad, toda vez que basta el simple acceso para consumar el delito. La tentativa es admisible.

Consideramos que existen una serie de artículos de la ley penal que se encuentran vinculados, pero hacen referencia a un exceso en la autorización para el acceso de datos, y no al acceso en sí.

El art 157 del CP reza: *"Será reprimido con prisión de un (1) mes a dos (2) años e inhabilitación especial de un (1) a cuatro (4) años, el funcionario público que revelare hechos, actuaciones, documentos o datos, que por ley deben ser secretos."*

[14] ¿Qué es el Phishing? (01 de septiembre de 2016). IntraMed. Recuperado de: https://www.intramed.net/contenidover.asp?contenidoid=64604

[15] Albors J. (30 de marzo de 2020). SIM swapping: qué es y cómo funciona este fraude. Welivesecurity. Recuperado de: https://www.welivesecurity.com/la-es/2020/03/30/que-es-sim-swapping-como-funciona/

El bien jurídico al decir de Riquert (2016, 3) es *"una faceta de la 'intimidad', es el 'secreto', pero no cualquiera sino el que tiene origen y debe mantenerse dentro del ámbito de la administración pública"*. Respecto de la acción típica, debe consistir en "revelar" un dato a terceros, hacerle saber de un conocimiento que está privado a estos últimos y que es obligación (por ley) del funcionario mantenerlo en el secreto. Según Donna (haciendo referencia a Solsona) *"La acción no consiste en 'divulgar', sino en 'revelar' que, si bien va más allá de comunicar, no implica publicar"* (2011, 449).

En cuanto al tipo subjetivo, el delito es doloso de dolo directo, toda vez que el funcionario público, en razón de su cargo conoce, y bien, las consecuencias de la violación de esta especial clase de secretos.

Autor sólo puede serlo quien reviste la calidad de funcionario público (delito especial propio). Es un delito de pura actividad, que se consuma con la revelación del dato. La tentativa es admisible, la cual podría consistir en el envío de un mensaje vía chat al destinatario, y que no llega por una interrupción proveniente del servidor del programa de mensajería.

Asimismo, la revelación también puede alcanzar a bancos de datos personales, de acuerdo con nuestra ley penal. El art. 157 bis, inc. 2, establece en este sentido que:

"Será reprimido con la pena de prisión de un (1) mes a dos (2) años el que: …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."

El bien jurídico es la intimidad de los datos personales. Las acciones típicas, en el inc. 2 son dos. La primera es revelar (explicación a la cual me remito a la dada por el art. 157 CP), concretamente respecto a datos que se encuentren en bases de datos personales. La segunda es proporcionar, entendida como la entrega de un dato a quien lo necesite, pudiendo consistir en una transferencia de archivos conteniendo la información privada. Para Riquert (2014, 13) la conducta del inc. 2 sería admisible a título de dolo eventual. En cambio, para Donna (2011, 453), no sería admisible el dolo eventual "debido a su redacción".

En cuanto a la autoría, la normativa establece que solo quien estuviere obligado a preservar el secreto será autor, por lo que se trata de un delito especial propio. El delito se consuma con la revelación de la información secreta, siendo admisible la tentativa. Imaginemos el caso de un funcionario de la AFIP que remita información secreta de un administrado a otro sujeto, enviando la misma en un archivo vía

WhatsApp. Sin embargo, el archivo que contenía los datos no se abrió debido a un desperfecto en el móvil del receptor.

VI.- Interceptación ilícita

El art. 153 del CP establece que: *"…Será reprimido con prisión de quince (15) días a seis (6) 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 o captare comunicaciones electrónicas o telecomunicaciones provenientes de cualquier sistema de carácter privado o de acceso restringido. La pena será de prisión de un (1) mes a un (1) 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…".*

Este artículo refleja una respuesta del Estado argentino a las previsiones del art. 3 del CB, en la lucha por evitar toda interceptación malintencionada de comunicaciones entre usuarios:

"…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 comunicados en transmisiones no públicas efectuadas a un sistema informático, desde un sistema informático o dentro del mismo, incluidas las emisiones electromagnéticas procedentes de un sistema informático que contenga dichos datos informáticos. Cualquier Parte podrá exigir que el delito se haya cometido con intención delictiva o en relación con un sistema informático conectado a otro sistema informático…"

El bien jurídico que se busca proteger, al igual que los demás tipos penales del capítulo III, es la intimidad (art. 18 y 19 de la CN). Concretamente se busca sancionar toda forma de violación a la privacidad de las personas que fueran afectadas en sus comunicaciones electrónicas, e- mails, videoconferencias, etc.

En cuanto a las acciones típicas, los dos primeros verbos típicos del primer párrafo (abriere o accediere) hacen referencia al acto de ingreso a la comunicación sin consentimiento de su titular. El fin se proyecta a violar la privacidad respecto del contenido de un correo o comunicación. Luego, se establece como conducta prohibida el apoderamiento de una comunicación electrónica, pudiendo dicho

concepto abarcar mucho más que la toma de dicho elemento ajeno para su disposición. En este sentido, el autor podría apropiarse, en razón de la cualidad virtual de la comunicación, clonando la misma, sin que su dueño siquiera se enterara.

Termina el párrafo con la supresión o desviación indebida. Ambas conductas importan una interrupción en la traslación de la comunicación de un punto a otro, sin el consentimiento de su correspondiente destinatario. Esto último surge de la descripción típica, cuando aclara que debe ser una comunicación *"que no le esté dirigida"* (todas las comunicaciones que desvíe su mismo titular antes de que las reciba son atípicas). La conducta puede consistir en un desvió de la comunicación a la cuenta del autor o de un tercero, o en la eliminación del elemento durante su traslación a destino.

La norma también prevé la interceptación o captación indebida de comunicaciones de sistemas privados o de acceso restringido. El tipo penal consiste en un monitoreo de carácter constante de la información que se envíe o reciba de un punto a otro (videoconferencia, chat, correo electrónico, etc.). Riquert (2013, 27) afirma que *"…A diferencia del supuesto de acceso donde se averigua el contenido de un mensaje, aquí el sujeto cuenta con un dispositivo que le permite conocer todos los mensajes que entran y salen, o escuchar las comunicaciones de una línea intervenida o leer el tráfico de despachos telegráficos"*…. Aporta asimismo el autor un dato respecto a quienes son los habituales infractores de la norma penal: *"Desde el punto de vista criminológico suele tratarse de autores que poseen conocimientos técnicos, que cuentan con cierta infraestructura, alentados por objetivos de espionaje (empresarial, político, etc.), utilizando los datos para negociar o realizar inteligencia diversa."*

Los agravantes que establece el artículo son dos. En primer lugar, cuando el autor, además de realizar las conductas mencionadas anteriormente, comunicare o publicare lo obtenido por su intervención. La comunicación implica dar a conocer la información a un número determinado de personas, en cambio, la idea de publicación implica una difusión a un número indeterminado de éstas. Coincidimos con Riquert (2013, 27) al entender que *"comunicar",* quiere decir *"hacer conocer a un tercero que no participa del delito el contenido de la correspondencia"*. En cuanto al segundo supuesto, se expresa la ley penal agravando la pena del delito si el autor es funcionario público. Ello opera como un límite al poder estatal en favor de la reserva de las acciones privadas de los ciudadanos.

En el tipo subjetivo, estos hechos son de carácter doloso, de dolo directo, viniendo a reforzar esa idea el elemento normativo *"indebido"*. Sin embargo, en algunos tipos como la comunicación o la publicidad, admitirían el dolo eventual.

En cuanto a la autoría, cualquier sujeto puede ser autor de estos hechos, salvo el caso del último párrafo, donde se prevé una figura agravada cuando el autor posea una especial cualidad, configurando un delito especial impropio. Son delitos de resultado, que admiten tentativa (ejemplo: el sujeto pasivo elimina su buzón de correo, previo al acceso de la correspondencia, o borra ésta última antes de que el autor la clone).

Si bien el delito en trato se consuma con la interceptación, podemos afirmar que la ley penal local a su vez regula otras conductas que podrían considerarse (no en forma necesaria) abarcadas en la etapa de agotamiento del plan criminal del autor.

En este sentido, el art. 155 CP establece la publicación abusiva de una comunicación electrónica no autorizada:

"*Será reprimido con multa de pesos un mil quinientos ($ 1.500) a pesos cien mil ($ 100.000), 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 pudiere causar perjuicios a terceros".*

Como bien jurídico se considera a la libertad del individuo de disponer de su intimidad, de dar a conocer a quien desee determinada información del cual es propietario.

La acción típica consiste en hacer público (por sí o por tercero) una comunicación electrónica (Email, SMS, WhatsApp, Hangouts, Signal, etc.) que estuviera en poder del autor, causando perjuicio a terceros.

Respecto del tipo subjetivo, según Donna (2011, 435) es un delito doloso, de dolo directo. La norma exige una intención determinada en razón del elemento normativo "indebidamente": *"el agente no debe tener derecho para hacerlo o no contar con autorización de quien sí lo tiene"* (Riquert, 2013, 4).

Por su parte, autor sólo puede serlo quien es poseedor de la correspondencia no destinada a publicidad. Es un delito de resultado que admite la tentativa.

Además de la normativa expuesta, es importante en este punto enunciar al art. 197 del CP, el cual aborda la interrupción o entorpecimiento de una comunicación telefónica o telegráfica. La normativa reza lo siguiente: *"Será reprimido con prisión de seis (6) meses a dos (2) años, el que interrumpiere o entorpeciere la comunicación telegráfica, telefónica o de otra naturaleza o resistiere violentamente el restablecimiento de la comunicación interrumpida".*

El bien jurídico protegido es la seguridad en el funcionamiento en los servicios de comunicaciones (de cualquier naturaleza). Esto incluye a empresas eminentemente privadas, cuando sus servicios son utilizados por un número indeterminado de personas.

Las acciones típicas se dividen, por un lado, en la *"interrupción"* o *"entorpecimiento"*, y por otro lado en *"resistir violentamente"*. La interrupción consiste en detener la continuidad de la comunicación en curso (Donna, 2011, 147), mientras que el entorpecimiento consiste en causar dificultades a la ejecución de la comunicación. Resistir violentamente implica la evitación del restablecimiento de la comunicación, instando activamente en el mantenimiento del estado de interrupción.

En cuanto a lo subjetivo, el delito es de carácter doloso. DONNA (2011, 148) y admite la posibilidad de dolo eventual. Para Núñez (2008, 322), habrá que diferenciar el elemento subjetivo entre interrupción o entorpecimiento de resistencia, siendo los primeros pasibles de dolo eventual, en tanto para los segundos solo puede ser posible el dolo directo.

Cualquier sujeto puede ser autor, no exigiendo la norma condiciones especiales. Mientras que los delitos de interrupción o entorpecimiento son de resultado y admiten tentativa, los actos de resistencia son de pura actividad, y no admiten la tentativa (Núñez, 2008, 323).

VII.- Ataques a la integridad de los datos y del sistema

El art. 157 bis, inc. 3, establece:

"Será reprimido con la pena de prisión de un (1) mes a dos (2) años el que: … 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 (1) a cuatro (4) años".

Tanto este artículo, como los que infra se detallan, encuentran su vinculación con el convenio de Budapest mediante el art. 4, el cual reza:

"…1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de actos que dañen, borren, deterioren, alteren o supriman datos informáticos.

2. Cualquier Parte podrá reservarse el derecho a exigir que los actos definidos en el apartado 1 provoquen daños graves…".

El bien jurídico es la integridad de los datos personales. La conducta típica del inc. 3, *"insertare o hiciere insertar"*, consiste en incorporar, incluir datos (por sí o por tercero) a una matriz de datos personales. El dato respecto de la veracidad del dato es irrelevante. Resulta interesante mencionar el comentario de Riquert (2014, 3) respecto de la nueva ubicación del tipo penal:

"Es claro entonces que se valora positivamente no sólo el apartamiento de la redacción consagrada por la LPDP Nº 25286, sino también la ubicación sistemática… de cara al bien jurídico protegido (honor, en su vertiente objetiva) podría darse el caso que el dato falso no lo lesionara ni lo pusiera en peligro. Incluso, podría pasar lo contrario, es decir, el dato falso mejorara su crédito o fama".

Respecto del tipo subjetivo, se exige (en virtud de los elementos normativos que se incorporan: *a sabiendas, ilegítimamente*) el dolo directo.

El autor puede serlo cualquier persona, salvo para el agravante del último párrafo, en el cual se aplica mayor punición cuando el sujeto activo es funcionario público (delito especial impropio). Son delitos de resultado y admiten tentativa. Puede ocurrir que durante la inserción del dato y antes de procederse al guardado del registro (para que impacte la incorporación del nuevo dato), el autor sea descubierto por el administrador en un monitoreo del sistema o por un superior en caso de un funcionario.

Por otro lado, el art 183 CP, en lo pertinente, impone:

"…Será reprimido con prisión de quince días a un año …el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos…".

Mientras que el art. 184 CP establece:

"…La pena será de tres (3) meses a cuatro (4) años de prisión, si mediare cualquiera de las circunstancias siguientes:

…5. Ejecutarlo en archivos, registros, bibliotecas, museos o en puentes, caminos, paseos u otros bienes de uso público; o en tumbas, signos conmemorativos, monumentos, estatuas, cuadros u otros objetos de arte colocados en edificios o lugares públicos; o en datos, documentos, programas o sistemas informáticos públicos;

6. Ejecutarlo en sistemas informáticos destinados a la prestación de servicios de salud, de comunicaciones, de provisión o transporte de energía, de medios de transporte u otro servicio público…".

Los artículos referidos no solo abordan formas de ataque a la integridad de datos (coincidiendo con las previsiones del art. 4 CB), sino que también los ciberataques a la integridad de sistemas informáticos. Ello también tiene un correlato en el CB, concretamente en el art. 5, el cual establece que:

"…Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático mediante la introducción, transmisión, provocación de daños, borrado, deterioro, alteración o supresión de datos informáticos…".

Respecto del bien jurídico, antes de la incorporación del segundo párrafo del referido art. 183, los bienes susceptibles de valor bajo una forma virtual carecían de una específica protección jurídica. Hoy dicha tutela se ha ampliado, preservándose de este modo la propiedad de aquellos datos y sistemas de carácter informático. La protección jurídico penal recae no solo sobre la propiedad de los elementos lógicos, como ser archivos, programas, bases de datos, sistemas operativos, etc., sino también sobre recursos físicos, como discos rígidos, soportes magnéticos de almacenamiento de datos similares (pendrives, discos externos, etc.), de cualquier forma de actividad que signifique un daño para estos.

Hay un gran número de conductas típicas. Respecto de la primera parte del párrafo analizado, cuando hace referencia a *"alterar"*, ello indica modificar su contenido o su estructura interna, *"destruir"* implica arruinar el elemento (en relación con su estado óptimo), e *"inutilizar"* importa tornar al archivo o programa incapaz de efectuar las tareas por las que fue creado.

Podemos mencionar en este campo la actividad de los llamados Crackers o Sombreros Negros[16], usuarios malintencionados que emplean fuerza bruta mediante determinados malwares, pero no solo para simplemente acceder o demostrar vulnerabilidades en sistemas sin autorización como lo suelen hacer los hackers, sino para destruir, robar, o inutilizar archivos y sistemas, a veces para beneficio propio o simplemente para divertirse. Así, mediante el "ransomware"[17], se han inutilizado

[16] González Y. (4 de septiembre de 2020). Cracker informático. ¿Es lo mismo que un hacker?. Grupo Atico34. Recuperado de: https://protecciondatos-lopd.com/empresas/cracker-informatico/

[17] Ramírez H. (11 de agosto de 2021). Ransomware: Definición, tipos y tendencias 2021-2022. Grupo Atico34. Recuperado de: Ransonware: Definición, tipos y tendencias 2024 | Grupo Atico34 (protecciondatos-lopd.com)

sistemas enteros tornando imposible su recuperación debido al cifrado que se aplica en los mismos.

Consideramos que el apoderamiento abusivo de datos de manera remota-online, debería ingresar en el marco de la estafa informática (art. 173 inc. 16), pues en aquellos casos se advierte la existencia de un ardid o engaño (por ejemplo: descarga de un software que se muestra como inocuo para la ciberseguridad) y luego, a partir de la activación del malware encubierto, comienza la manipulación remota de un sistema informático y/o de los datos que en dichos equipos se encuentran, afectando el patrimonio de la víctima.

Al agravante del artículo 184, se le incorpora estas particulares formas de afectación a la propiedad en el universo informático, cuando el acto recaiga sobre elementos lógicos o sistemas informáticos pertenecientes al Estado, o bienes de uso público.

En cuanto al tipo subjetivo, las conductas descritas son dolosas, de dolo directo.

Respecto de la autoría, cualquier persona puede ser autor, no se exigen condiciones especiales. Son delitos de resultado, toda vez que se da una transformación del elemento lógico, mediante las conductas descriptas supra. La tentativa es admisible.

VIII.- Abuso de los dispositivos

La segunda parte del segundo apartado del art. 183 del CP establece que sufrirá la pena de prisión de quince días a un año, el que: *"…vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños…".*

Aquí, a diferencia del apartado anterior, no se sanciona el daño en sí, sino las conductas anteriores a dicha afectación. Este fragmento tiene una relación estrecha con las previsiones del CB en su art. 6, el cual dicta lo siguiente:

"…1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de los siguientes actos:

a) La producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de:

i) Un dispositivo, incluido un programa informático, diseñado o adaptado principalmente para la comisión de cualquiera de los delitos previstos de conformidad con los anteriores artículos 2 a 5;

ii) Una contraseña, un código de acceso o datos informáticos similares que permitan tener acceso a la totalidad o a una parte de un sistema informático, con el fin de que sean utilizados para la comisión de cualquiera de los delitos contemplados en los artículos 2 a 5…"

La mera posesión de estos elementos para acceder a sistemas (6.1.b del CB) no es aplicable en nuestro país, conforme la reserva efectuada en la ley 26.411, por exigir la normativa internacional una tipificación de actos preparatorios y una consecuente anticipación de la pena. Para nuestro país, según reza la normativa local, sería este concepto "ajeno a su tradición legislativa en materia jurídico penal". Consideramos que el fundamento es muy escueto y superficial, sobre todo existiendo tipos penales de tenencia en nuestro sistema legal (art. 14 de la ley 23.737 que regula la tenencia simple, por ejemplo). Sin perjuicio ello, lo expresado en el art. 2.a de la ley de aprobación del CB anula toda forma de tenencia de dispositivos, programas o datos para acceder (art. 2 CB), interceptar (art. 3 CB) o dañar (arts. 4 y 5 CB).

El apartado de la normativa del 183 CP toma como una conducta típica el *"vender"*, consistente en realizar actos de comercio con relación a estos objetos dañinos. Luego continúa con *"distribuir"*, que implica poner el programa o archivo a disposición de terceros. *"Hacer circular"* es propagar el elemento hacia otros sistemas informáticos (virus, troyanos, etc.). Y por último *"introducir"*, que hace referencia a la colocación del programa en un ordenador para causar daños.

En cuanto al tipo subjetivo, las conductas descritas son dolosas, admitiendo dolo eventual.

Sujeto activo como pasivo pueden serlo cualquier persona, no se exigen condiciones especiales. Son delitos de pura actividad, toda vez que implican la mera realización de las conductas descriptas para consumar el delito, sin necesidad de transformación alguna en elemento lógico concreto. La tentativa es admisible, un ejemplo de esto sería: una persona recibe del autor un pendrive, el cual contiene archivos de interés para el primero (además de un virus autoejecutable con la virtualidad te tornar inutilizable cualquier ordenador), pero antes de insertar el dispositivo de almacenamiento, la notebook queda sin batería, o es interrumpida la acción por un tercero que le avisa las intenciones del sujeto activo.

IX.- Falsificación informática

La ley de delitos informáticos no regula esta especie de conductas. Sin embargo, entendemos que ello se debe a que, con la modificación del art. 77 del CP, toda referencia a los documentos altera, a su vez, el alcance de los delitos contra la fe pública. Ello se evidencia sobre todo en lo referido a la falsificación de documentos en general.

Consideramos que el análisis dogmático de todo el Capítulo III, del Título XII del Código Penal, excede al presente artículo por la amplitud que merece su desarrollo. Sin embargo, podemos afirmar de la lectura de dicho capítulo que existe una vinculación clara con el art. 7 del CB, el cual establece la falsificación informática: *"…Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno, cuando se cometa de forma deliberada e ilegítima, la introducción, alteración, borrado o supresión de datos informáticos que dé lugar a datos no auténticos, con la intención de que sean tenidos en cuenta o utilizados a efectos legales como si se tratara de datos auténticos, con independencia de que los datos sean o no directamente legibles e inteligibles. Cualquier Parte podrá exigir que exista una intención fraudulenta o una intención delictiva similar para que se considere que existe responsabilidad penal...".*

Es evidente que el "dato" al que se refiere el art. 7 del instrumento internacional se refiere a aquellos que tienen el carácter de documento para la ley penal, pues de la normativa del convenio, surge una finalidad requerida al autor dirigida a buscar que se tengan como "auténticos" a los fines legales, aquellos "datos" que no lo son.

X.- Estafa informática

El art. 173 CP dispone:

"Sin perjuicio de la disposición general del artículo precedente, se considerarán casos especiales de defraudación y sufrirán la pena que él establece:

…15. 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.

16. 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".

Este artículo encuentra relación con las previsiones del art. 8 del CB, el cual reza:

"…Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno los actos deliberados e ilegítimos que causen un perjuicio patrimonial a otra persona mediante: a) Cualquier introducción, alteración, borrado o supresión de datos informáticos; b) cualquier interferencia en el funcionamiento de un sistema informático, con la intención fraudulenta o delictiva de obtener ilegítimamente un beneficio económico para uno mismo o para otra persona…".

El bien jurídico que busca protegerse es la propiedad, respecto de cualquier acto que importe una producción de perjuicio patrimonial a terceros, y un beneficio para quien lo produzca, mediante la utilización de medios informáticos.

El inc. 15 no fue incorporado por la ley 26.388, sino por la ley 25.930 de reforma del CP, sancionada el 25 de agosto de 2004. De igual forma entendemos que es un delito que debe ser considerado en virtud del medio en que se actúa, el cual puede ser virtual (falsificación de tarjeta mediante duplicación, utilización de ingeniería social para la extracción o transferencia de dinero por cajeros automáticos mediante el empleo de tarjetas, etc.), y las consecuencias que produce a nivel global respecto de sus usuarios.

Establece como conducta típica el *"usar"*, es decir dar empleo de la tarjeta de compra, crédito o débito, conforme a su función (compra de bienes, extracción de dinero etc.). Según Aboso y Zapata (2006, 78) *"esta norma prevé un amplio abanico de modalidades delictivas (hurto, robo, falsificación, engaño, etc.), que sirvan como vehículo para que el autor utilice de manera fraudulenta una tarjeta de compra…incluso mediante el uso no autorizado de datos".*

En cuanto a lo subjetivo, es un delito doloso de dolo directo.

Autor puede ser cualquier persona. Para su consumación debe existir un ardid o engaño sobre la víctima y un beneficio económico subsecuente para el autor, en virtud de ello se afirma que es un delito de resultado y que su tentativa es admisible (al momento de usar la tarjeta su verdadero titular bloquea para consumos la misma al advertir que se hallaba perdida).

El inc. 16 establece como conducta típica el "defraudar", es decir causar un perjuicio patrimonial con un beneficio económico subsecuente, mediante ardid o engaño, mediante el empleo de técnicas de manipulación informática. Hasta la incorporación de este artículo, se entendía que las máquinas no podían ser engañadas, por ende, no pasibles de ser "estafadas". Actualmente queda claro que, si el acto de perjuicio patrimonial se efectúa alterando el sistema informático, esas

conductas que antes se tomaban como atípicas, hoy cobran relevancia jurídico penal. Se afecta la seguridad del sistema mediante tecnología creada a este efecto (programas de infiltración a cuentas bancarias, utilización de ingeniería social y hacking, phishing simulando la página de home banking para obtener contraseñas, etc.).

En cuanto al tipo subjetivo, es un delito doloso, de dolo directo.

Cualquier persona puede ser autora del delito. Es un delito de resultado material, toda vez que se produce un perjuicio patrimonial como fruto de la manipulación. Admite tentativa. Por ejemplo: El autor ingresa al home banking de la víctima y transfiere los fondos a otra cuenta, pero antes de retirar la suma obtenida en el cajero, el banco advierte la operación fraudulenta a partir de la denuncia de la víctima y anula la transferencia.

XI.- Pornografía infantil

El art. 128 del CP establece:

"…Será reprimido con prisión de tres (3) a seis (6) años el que produjere, financiare, ofreciere, comerciare, publicare, facilitare, divulgare o distribuyere, por cualquier medio, toda representación de un menor de dieciocho (18) años dedicado a actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales, al igual que el que organizare espectáculos en vivo de representaciones sexuales explícitas en que participaren dichos menores.

Será reprimido con prisión de cuatro (4) meses a un (1) año el que a sabiendas tuviere en su poder representaciones de las descriptas en el párrafo anterior. Será reprimido con prisión de seis (6) meses a dos (2) años el que tuviere en su poder representaciones de las descriptas en el primer párrafo con fines inequívocos de distribución o comercialización. Será reprimido con prisión de un (1) mes a tres (3) años el que facilitare el acceso a espectáculos pornográficos o suministrare material pornográfico a menores de catorce (14) años. Todas las escalas penales previstas en este artículo se elevarán en un tercio en su mínimo y en su máximo cuando la víctima fuere menor de trece (13) años…".

Este artículo se vincula con el art. 9 del CB, el cual reza en lo pertinente que:

"…1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de los siguientes actos:

a) La producción de pornografía infantil con vistas a su difusión por medio de un sistema informático;

b) la oferta o la puesta a disposición de pornografía infantil por medio de un sistema informático;

c) la difusión o transmisión de pornografía infantil por medio de un sistema informático,

d) la adquisición de pornografía infantil por medio de un sistema informático para uno mismo o para otra persona;

e) la posesión de pornografía infantil en un sistema informático o en un medio de almacenamiento de datos informáticos…".

Si bien no se mencionan en el art. 1 del CB, lo cierto es que el tratado continúa ofreciendo definiciones en el artículo 9. En este caso, son específicas de la cuestión vinculada a los delitos de pornografía infantil en el ámbito virtual:

"…2. A los efectos del anterior apartado 1, por «pornografía infantil» se entenderá todo material pornográfico que contenga la representación visual de:

a) Un menor comportándose de una forma sexualmente explícita;

b) una persona que parezca un menor comportándose de una forma sexualmente explícita;

c) imágenes realistas que representen a un menor comportándose de una forma sexualmente explícita.

3. A los efectos del anterior apartado 2, por «menor» se entenderá toda persona menor de dieciocho años. No obstante, cualquier Parte podrá establecer un límite de edad inferior, que será como mínimo de dieciséis años…".

Es importante resaltar, que la ley de aprobación del CB hizo reservas de aplicación a este artículo del instrumento internacional. En este sentido, el art. 2 inc. b, indica que:

"…La REPÚBLICA ARGENTINA hace reserva de los artículos 9.1.d., 9.2.b. y 9.2.c. del CONVENIO SOBRE CIBERDELITO y manifiesta que estos no regirán en su jurisdicción por entender que son supuestos que resultan incompatibles con el CÓDIGO PENAL vigente, conforme a la reforma introducida por la ley 26.388…".

En consecuencia, y de acuerdo con esta normativa, la adquisición de pornografía infantil para sí o para otra persona no es punible en forma expresa en nuestro derecho salvo en los casos del tercer párrafo del 128, cuando la facilitación a espectáculos o el suministro de material se realice a favor de un menor de catorce (14) años. Asimismo, de acuerdo con la ley de aprobación del convenio, solamente ingresaría en el concepto de pornografía infantil el material pornográfico vinculado a menores comportándose de manera sexualmente explicita, no así cuando sean personas que parezcan menores o sean representaciones realistas de aquellos.

El artículo 2 inc. c de la ley 27.411, sin embargo, establece una reserva parcial del art. 9.1.e del CB, por lo que la mera posesión de material pornográfico sobre menores tampoco sería punible en nuestro sistema legal, *"…cuando la posesión allí referida fuera cometida con inequívocos fines de distribución o comercialización (artículo 128, segundo párrafo, del CÓDIGO PENAL)…"*. Esto era así hasta el año 2018, cuando mediante una nueva reforma legislativa (Ley 27.436), implícitamente el legislador negó la reserva hecha en 2017, incorporando la tenencia dolosa de pornografía infantil al artículo 128 del CP. Por ende, en nuestro país también es punible la tenencia dolosa. Esta normativa no solo modificó las conductas típicas del 128 CP, sino que también aumentó sus escalas penales considerablemente, además de incorporar un agravante genérico por la edad de la víctima.

El bien jurídico que este tipo penal pretende proteger es la indemnidad sexual del menor.

En cuanto a las conductas típicas, si bien el primer párrafo del artículo 128 ya regulaba la publicación o producción de imágenes y espectáculos pornográficos de menores, la modificación de la ley 26.388 amplía el número de conductas típicas. En la anterior redacción se debía producir o publicar. El nuevo artículo va más allá, atendiendo a las nuevas formas de tráfico de información propia de las redes de pedofilia. En un aspecto inicial, sanciona la etapa de creación del material pornográfico infantil (producción, financiamiento), y luego sigue con su puesta en circulación (ofrecimiento, comercio, publicación, facilitación, divulgación o distribución). También sanciona la organización de espectáculos en vivo de contenido explícito, donde intervengan menores.

La ley prevé no sólo imágenes (como indicaba la anterior redacción), sino *"toda representación"* para captar videos, fotos, retransmisión o streaming en vivo, etc., o las formas que surjan en el futuro. Además, aclara que dichas representaciones deben ser de un menor de 18 años, tope establecido por nuestra legislación civil, el CB y la

Convención sobre los Derechos del Niño, teniendo esta última jerarquía constitucional en virtud de los establecido en el art. 75 inc. 22 CN. Dicha representación debe incluir *"actividades sexuales explícitas -donde aparezcan menores- o toda representación de sus partes genitales con fines predominantemente sexuales"*.

En cuanto al elemento subjetivo, son delitos dolosos. Consideramos que en todos los casos sólo puede admitirse el dolo directo. Riquert (2013, 25) considera que las conductas pueden admitir el dolo eventual, salvo en el tercer párrafo debido a la ultraintención que requiere la norma. A su vez, pone de relieve la posibilidad de error de tipo acerca de la edad del menor en las figuras mencionadas, toda vez que no existe figura culposa.

De acuerdo con Riquert (2013, 19), las conductas típicas mencionadas al inicio del primer párrafo, como la de organizar espectáculos en vivo, son comportamientos activos, de resultado e instantáneo, de pluralidad de actos, también denominado mixto alternativo.

En cuanto a la autoría, estos hechos pueden ser cometidos por cualquier persona, y no hay obstáculo alguno para que se apliquen las reglas de la participación criminal. En cuanto a la víctima, solo puede ser un menor de 18 años para encontrarse en el ámbito de lo prohibido por la norma penal. En lo que refiere a la tentativa, las conductas del primer párrafo admitirían el instituto.

Se pueden pensar varios casos de tentativas del primer supuesto. Ejemplo: imaginemos que el autor sube el archivo prohibido en una cuenta en la nube de acceso restringido, bastando con acceder a la misma para proceder a la descarga. En ese caso si el autor ha entregado a sus clientes el link de la cuenta donde deben ingresar, un acto de tentativa importaría el acto de subir el archivo, produciéndose a posteriori la imposibilidad de acceso a los datos porque el mismo proveedor del servicio ha bloqueado el archivo y por ende los links enviados nunca funcionaron (tentativa de publicación).

En el segundo párrafo, basta con probar la simple tenencia para consumar el tipo, sin perjuicio podría admitir tentativa. Así, el autor puede ser sorprendido al momento de sacar de un sobre un pendrive que porta el material prohibido. En el tercer párrafo, lo que interesa aquí es que tenga predominantemente esa finalidad, caso contrario, de no probarse tal extremo (el cual debe ser inequívoco, como se ha afirmado supra), la conducta se desplazaría al segundo párrafo. La tenencia culposa es atípica.

Las cuestiones atinentes a la perseguibilidad y comprobación de estos actos son en extremo complejas. Esto puede llevarnos a pensar que, con el afán de capturar al autor, se realicen actos encubiertos (infiltración en la computadora, portátil, celular, o la utilización de agentes provocadores, etc.) que afectarían el ámbito de intimidad del autor (art. 19 CN.), entre otras consecuencias en el plano constitucional.

En cuanto al cuarto párrafo, la facilitación al acceso es un delito de pura actividad, consistente en un aporte o ayuda para el acceso, por lo que se consuma con esa sola conducta. La tentativa es admisible. Imaginemos que el autor envía un link a un menor de 14 años, vía WhatsApp, para ver un espectáculo pornográfico en vivo online mediante plataforma streaming, el cual no se produce al día y hora del evento por problemas del servidor.

Es importante resaltar, que la norma prevé en su último párrafo un agravante para todos los delitos existentes en los primeros cuatro párrafos del 128 CP, cuando la víctima sea un menor de trece (13) años.

XII.- Propiedad intelectual

La propiedad intelectual se encuentra protegida por la ley 11.723, la cual también incluye datos o software (programas, sistemas operativos, obras audiovisuales, literarias, artísticas, científicas, etc.). Mediante la distribución no autorizada de los mismos a través de determinadas redes P2P, Torrent, etc., se afectan los derechos de sus autores, produciéndoles pérdidas increíbles en términos económicos a nivel global.

Este artículo se vincula con las previsiones del art. 10 del CB, el cual establece que:

"…1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno las infracciones de la propiedad intelectual, según se definan en la legislación de dicha Parte, de conformidad con las obligaciones asumidas en aplicación del Acta de París de 24 de julio de 1971 por la que se revisó el Convenio de Berna para la protección de las obras literarias y artísticas, del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del Tratado de la OMPI sobre la propiedad intelectual, a excepción de cualquier derecho moral otorgado por dichos Convenios, cuando esos actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático. 2. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno las infracciones de los derechos afines definidas en la legislación de dicha Parte, de conformidad con las obligaciones que ésta haya asumido en aplicación de la Convención

Internacional sobre la protección de los artistas intérpretes o ejecutantes, los productores de fonogramas y los organismos de radiodifusión (Convención de Roma), del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del Tratado de la OMPI sobre las obras de los intérpretes y ejecutantes y los fonogramas, a excepción de cualquier derecho moral otorgado por dichos Convenios, cuando esos actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático…".

El bien jurídico de estos delitos es la protección de la propiedad inmaterial del autor respecto de determinadas obras de carácter literarias, científicas, musicales, artísticas, así también como la titularidad de patentes, marcas, etc., poseyendo estos bienes un valor pecuniario y afectivo para quien sea su dueño.

En cuanto a las conductas típicas, las cláusulas penales se encuentran en dicha ley, desde el art. 71 a 78, prohibiendo las conductas de "piratería". Estas abarcan la apropiación, distribución, reproducción, edición o venta de obras, programas o sistemas operativos, que gozan de derechos de autor, a personas no autorizadas por este último.

Respecto del elemento subjetivo, son conductas compatibles con el dolo directo, toda vez que el autor necesariamente conoce y tiene la voluntad de desplegar las conductas supra referidas al momento de hacerlas, advirtiendo un beneficio económico en ello (compra a un precio excesivamente inferior o adquisición gratuita, venta a terceros sin autorización del titular de la obra, etc.). Es de destacar la opinión de Carnevale (2008, 6) respecto al carácter de estas conductas (socialmente aceptables para este último):

"…La gran cantidad de personas que en forma habitual descargan temas musicales de Internet ha llevado a cuestionar la propia legislación en materia de derechos intelectuales. Más aún, hay quienes llegan a considerar que, dado que se trata de una práctica de difusión masiva que adquirió una habitualidad socialmente aceptada, no debería ser sancionada penalmente.

Puede uno preguntarse si no encontraría cabida en este nuevo paradigma cultural la "teoría de la adecuación social" que fuera desarrollada originariamente por Welzel. La misma considera que las acciones que se mueven funcionalmente dentro del orden históricamente constituido, es decir, que son socialmente adecuadas nunca caen dentro del tipo aun cuando con arreglo al tenor literal pudiesen ser subsumidas en él…".

Una cuestión sumamente interesante que excede el marco de este artículo.

XIII.- Conclusiones

Como se podrá apreciar del análisis que se ha efectuado de los delitos informáticos creados por la ley 26.388, el fenómeno abarca formas peculiares de afectación a bienes jurídicos como la intimidad o privacidad, la propiedad, la libertad, la indemnidad sexual, la seguridad pública, entre otros. Es palmaria la preocupación de los Estados del mundo con relación a la problemática, y el CB es el primer instrumento internacional que da una respuesta en cuanto al tratamiento que se debe dar a estos hechos.

El Convenio de Budapest cumplió en 2021 veinte años desde su creación. En este marco la Argentina como país signatario le ha dado respuesta penal al problema de la criminalidad digital, sin perjuicio de existir hechos pendientes de tratamiento, como ser la sustitución de identidad, las calumnias e injurias por internet, apología de delitos vía virtual, amenazas y coacciones a través de la web, etc.

El Anteproyecto de Código Penal de 2014 estableció previsiones más concretas respecto a la materia de delitos informáticos, estableciendo penas para el hacking simple y agravado (art. 123); la sustitución de identidad (ap. f art. 123); daño informático (art.161); violación de derechos intelectuales (art. 150), entre otros.

Actualmente existen una serie de proyectos ley para incorporar estos tipos legales, entre los que podemos citar al proyecto de incorporación del art. 139 ter sobre delito de suplantación o apoderamiento de identidad digital (03/03/2020): *"…Artículo 139 ter: Será reprimido con prisión de seis meses a dos años el que suplantare o se apoderare de la identidad de una persona humana sin su consentimiento, a través del uso de su nombre, apellido, foto o imagen, o cualquier otra característica que indefectiblemente la identifique como tal, utilizando para tal fin las Tecnologías de la Información y la Comunicación, causando un perjuicio a la persona cuya identidad se suplanta o a terceros. La pena será de prisión de uno a cuatro años, siempre y cuando no configure un delito más severamente penado, en los siguientes casos:*

a) Si se realizare de forma sostenida en el tiempo o de modo tal que obligare a la víctima a alterar su proyecto de vida;

b) Si la identidad creada, apropiada o utilizada fuere de una persona menor de 18 años…".

Cabe resaltar que, en materia de pornovenganza y violencia contra la mujer en medios digitales, recientemente se aprobó y promulgó la "Ley Olimpia" (27.736) la cual otorga amparo contra todo trato o acto violento hacia la mujer en ámbito digital. En tal sentido, esta normativa modificó la ley de protección integral contra las

mujeres (26.485), abarcando toda forma de violencia dirigida a la persona y/o bienes digitales de las mujeres, en su desenvolvimiento en el ciberespacio. En tal sentido toma medidas para el cese y/o remoción del acto lesivo:

"...Modifícase el apartado a.2. del artículo 26 de la ley 26.485, por el siguiente texto:

a.2. Ordenar al presunto agresor que cese en los actos de perturbación o intimidación que, directa o indirectamente, realice hacia la mujer, tanto en el espacio analógico como en el digital

...Incorpórase como apartado a.8. del artículo 26 de la ley 26.485, el siguiente texto:

a.8. Ordenar la prohibición de contacto del presunto agresor hacia la mujer que padece violencia por intermedio de cualquier tecnología de la información y la comunicación, aplicación de mensajería instantánea o canal de comunicación digital...".

Por último, establece la remoción digital de contenido que menoscabe la dignidad y la integridad de la mujer:

"...Incorpórase como apartado a.9. del artículo 26 de la ley 26.485, el siguiente texto:

...a.9. Ordenar por auto fundado, a las empresas de plataformas digitales, redes sociales, o páginas electrónicas, de manera escrita o electrónica la supresión de contenidos que constituyan un ejercicio de la violencia digital o telemática definida en la presente ley, debiendo identificarse en la orden la URL específica del contenido cuya remoción se ordena. A los fines de notificación de la medida del presente inciso se podrá aplicar el artículo 122 de la ley 19.550...".

Sin perjuicio de que las medidas antes expresadas importan un avance frente al flagelo de la violencia por medios digitales a la mujer, la misma no establece sanciones penales para el infractor. En este orden, actualmente se encuentra en trámite en el Congreso de la Nación la llamada "Ley Belén", que trata la "pornovenganza" (proyecto 2757-D-22), prohibiendo con pena de prisión varias modalidades y grados de afectación a la intimidad por medios virtuales:

"...Incorpórase el artículo 155 bis al Capítulo III del título V del Código Penal argentino, que queda redactado de la siguiente manera: Artículo 155° bis: Se aplicará prisión de tres meses a dos años y el doble de la multa establecida en el artículo 155° a quien, por cualquier medio, sin autorización de la víctima o mediando engaño, videograbe, audiograbe, fotografíe, filme o elabore, documentos con contenidos de desnudez, naturaleza sexual o representaciones sexuales explícitas.

Se aplicará prisión de tres meses a tres años y el doble de la multa establecida en el párrafo anterior a quien por cualquier medio, y sin autorización de la víctima, difunda, publique, envíe o

de cualquier manera ponga al alcance de terceros los documentos referidos en el párrafo anterior obtenidos con o sin mediar su consentimiento.

Se aplicará prisión de seis meses a tres años y el doble de la multa establecida en el primer párrafo a quien por cualquier medio, y sin autorización produzca y a posterioridad difunda, publique, envíe o de cualquier manera ponga al alcance de terceros los documentos referidos en el primer párrafo, obtenidos con o sin mediar consentimiento de la víctima.

Se aplicará prisión de un mes a dos años y el doble de la multa establecida en el art. 155 cuando los documentos que se elaboren, difundan, publiquen, envíen o de cualquier manera se pongan al alcance de terceros, no correspondan con la persona que es señalada e identificada en los mismos...".

Asimismo, el mencionado proyecto establece una modificación de los arts. 72 y 73 del CP, indicando que la acción penal para la persecución de los delitos abordados en el párrafo anterior será de oficio dependiente de instancia privada.

Es importante destacar que la investigación de estos hechos no es sencilla, toda vez que el agresor puede estar a miles y miles de kilómetros de distancia, cruzando las fronteras a países lejanos. Además, al moverse dentro de un mundo virtual, las huellas son sencillas de borrar, basta con presionar un botón.

Es dable destacar que respecto de estos delitos rige el principio de universalidad en razón de que estos actos afectan a la comunidad internacional, por ende, cualquier país afectado puede investigar estos hechos. Son competentes los fueros federales, pudiendo realizarse las denuncias por estos hechos ante la Unidad Fiscal Especializada en Ciberdelincuencia -UFEC- en CABA o cualquier fiscalía federal del interior del país. Si son delitos donde se ha afectado la información proveniente de un banco de datos personales, se debe acudir a la Dirección Nacional de Protección de Datos Personales. Inclusive existen ONG que facilitan información acerca de cómo actuar frente a estos delitos, además de brindar las direcciones y teléfonos de los lugares a donde acudir en estos casos[18].

Sin perjuicio de lo dicho, la competencia provincial es posible. En "Eslaiman"[19] la CSJN adhirió al dictamen del procurador general, en el marco de una contienda

[18] La ONG Argentina Cibersegura ofrece su portal para informar y colaborar a la víctimas de delitos informáticos que quieran efectuar denuncias: https://www.argentinacibersegura.org/noalgrooming/pdf/den uncia-delito-informatico.pdf.

[19] Dictamen del Procurador de la CSJN en "Eslaiman, Alicia s/infr. Ley 11.723" S.C. Comp. 888, L. XLV. 15/12/2009

negativa de competencia afirmando esta posibilidad. En el caso se determinó que, debido a que el IP del dispositivo que el autor empleó para enviar y vender una obra sin autorización de su titular, se encontraba dentro de la jurisdicción donde se encontraba su víctima, se estableció que la competencia le correspondía al juzgado provincial.

Sin embargo, en la causa D.S.D. la CSJN adhirió al dictamen del procurador general, entendiendo que la justicia federal es competente para actuar en el marco de una investigación por acceso no autorizado a cuentas ajenas de correo electrónico y de redes como Facebook. El procurador afirmó lo siguiente respecto de las cuentas de dichos servicios de internet: *"constituyen una "comunicación electrónica" o "dato informático de acceso restringido"*, en los términos de los artículos 153 y 153 bis del Código Penal, según la ley 26.388, cuyo acceso sólo es posible 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 (artículo 2º y 3º de la ley 19.798)"[20]

Sin lugar a duda, el ciberespacio se configura como un universo plagado de riesgos para la sociedad contemporánea. Por ello, es importante la colaboración entre los Estados, mediante la armonización legislativa en la materia y la existencia de tratados y convenios multilaterales.

No es una tarea sencilla, pero sin lugar a dudas la Argentina ha dado grandes pasos para alcanzar el fin que los países involucrados buscan, que es, como lo ha dicho Bert Koenders, ex ministro de relaciones exteriores de Holanda, en la IV Conferencia Global sobre el Ciberespacio celebrado en la Haya, los días 16 y 17 de abril de 2015, que el ciberespacio sea un lugar *"Libre, para que todo el mundo tenga acceso a Internet y las oportunidades sin precedentes que ofrece. Abierto, para que la información pueda fluir sin obstáculos entre los usuarios en un único ciberespacio, y seguro, porque los datos personales estén protegidos y la privacidad, salvaguardada"*[21].

XIV.- Bibliografía

- Aboso, G. E., Zapata, M. F. (2006). Cibercriminalidad y derecho penal. Editorial B de F.

[20] Dictamen del Procurador de la CSJN en "D. S. D. s/ violación correspondencia medios elect. art. 153 2°p" S.C. Comp. 778, L. XLIX. 24/06/2014

[21] Ballesteros C. (17 de abril de 2015). La metamorfosis del cibercrimen. El País. Recuperado de: http://internacional.elpais.com/internacional/2015/04/16/actualidad/1429210295_215966.html.

- Carnevale, Carlos A. (2008) ¿Es posible ser condenado penalmente por descargar música de internet? – Mp3, P2P, y garantías constitucionales. eldial.com. https://www.eldial.com/nuevo/lite-tcd-detalle.asp?id=3483&id_publicar=4418&fecha_publicar=12/03/2008&camara=Doctrina&base=50.
- Donna, E. (2011) Derecho Penal – Parte Especial. Tomo II-A. 2 ed. Rubinzal-Culzoni Editores.
- Donna, E. (2011) Derecho Penal – Parte Especial. Tomo II-C. 2 ed. Rubinzal-Culzoni Editores.
- Gutiérrez R., Radesca L. C. y Riquert M. A. (2013). Violación de secretos y de la privacidad. Revista Pensamiento Penal. http://www.pensamientopenal.com.ar/system/files/cpcomentado/cpc37762.pdf.
- Hertler, F. E. (2021). Ley penal y pedofilia en la red: pornografía infantil y child grooming en Argentina. Conexiones, 1(6), 161. http://ojs.ucp.edu.ar/index.php/conexiones/article/view/790.
- Núñez, R. (2008). Manual de derecho penal, parte especial. 3 ed. Lerner.
- Riquert, M. A. (2018). Código Penal de la Nación Comentado y Anotado (T.I-III). Erreius.
- Riquert, M. A. (2016). Revelación de hechos, actuaciones, documentos y datos secretos. Revista Pensamiento Penal. http://www.pensamientopenal.com.ar/system/files/art._157_revelacion_de_datos_secretos.pdf
- Riquert, M. A. (2014). Acceso ilegítimo a banco de datos personales, revelación ilegítima de su información e inserción ilegítima de datos. Revista Pensamiento Penal. http://www.pensamientopenal.com.ar/system/files/cpcomentado/cpc40204.pdf
- Riquert, M. A. (2013). Publicación ilegal de comunicaciones con otro destino. Revista Pensamiento Penal. http://www.pensamientopenal.com.ar/system/files/art.155_publicacion_indebida_de_correspondencia.pdf.
- Riquert, M. A.; Riquert, F. L. (2013) análisis del art. 128 del CP. Revista Pensamiento Penal. http://www.pensamientopenal.com.ar/system/files/cpcomentado/cpc37753.pdf
- Rubio, J. H. (2019). Internet y postmodernidad: un soporte de comunicación tan necesario como irreverente en la actualidad. Necesidades pedagógicas. Vivat Academia, (146), 21- 41. https://doi.org/10.15178/va.2019.146.21-41