CIBERDELITOS 2024: EL CONVENIO DE BUDAPEST Y SU INFLUENCIA EN EL DERECHO PENAL ARGENTINO

Facundo Emmanuel Hertler[1]
(Universidad Nacional del Nordeste, Corrientes, Argentina)

Fecha de recepción: 12/10/2021
Fecha de aceptación: 08/03/2024

Resumen: El presente artículo analiza el avance legislativo a nivel nacional y convencional en materia de ciberdelitos. Concretamente se toma al Convenio de Budapest como normativa de referencia, un documento internacional de más de dos décadas de existencia. 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 similitudes entre aquella y el Convenio de Budapest (con sus protocolos adicionales). A modo de conclusión, se hará una breve mención de las conductas que se encuentran pendientes de recepción por la ley penal.

Palabras claves: 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 existed for more than two decades, 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 (with its additional protocols) are determined. To conclude, the behaviors that are still pending of being provided by the criminal law are mentioned.*

Keywords: *Convention – Internacional – Cybercrimes – Argentina – Criminal Law.*

[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

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 objetos de protección de bienes jurídicos.

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 Tecnologías de la Información y de la Comunicación (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.

---

[2] Concepto de posmodernidad en 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] Concepto de TICs (05 de agosto de 2021). *Etecé*. Recuperado de: https://concepto.de/tics/

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

[5] Clasificación de malware en 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: http://www.telam.com.ar/notas/201705/189655-ciberataque-ransomware-wannacry.html.

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

II.- EL "CONVENIO DE BUDAPEST" COMO PRIMERA MANIFESTACIÓN INTERNACIONAL EN LA LUCHA CONTRA EL CIBERCRIMEN

En razón de 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 firmar el Convenio Sobre Ciberdelincuencia[8], siendo el primer tratado internacional que trata la cuestión, estableciendo definiciones concretas (Capítulo I); tipos penales específicos, reglas particulares para determinación de responsabilidad penal, herramientas determinadas de investigación, de obtención y conservación de prueba, cuestiones de jurisdicción (Capítulo II); reglas relativas a extradición y asistencia internacional entre los países signatarios (Capítulo III); y, por último, cláusulas vinculadas las formas y condiciones de adhesión al convenio y sus efectos en los países miembros, reservas, consultas, denuncias y solución de controversias (Capítulo IV). La bondad de este tratado, es que permite la incorporación de países no europeos a sus cláusulas, llegando a obtener un total de 69 ratificaciones y adhesiones[9].

A fin de demarcar las fronteras de extensión del presente artículo, cabe aclarar que solamente trabajaremos con el Capítulo I del Convenio de Budapest que aborda la terminología empleada en el instrumento internacional, para definir y comprender los institutos que trata. Posteriormente, analizaremos el Capítulo II, Sección I, que consagra dentro de las "medidas que deberán adoptarse a nivel nacional" a las normas de derecho penal sustantivo que deben legislar los países signatarios.

Dicha Sección del Capítulo II se divide en cinco títulos, agrupando los delitos en categorías basadas en los bienes que se afectan. El Título 1 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[10]).

Luego, en el Título 2, el instrumento internacional consagra los "*delitos informáticos*" abarcando a la falsificación informática y el fraude informático (arts. 7 y 8 CB).

Continúa con los llamados "*delitos relacionados con el contenido*" (Título 3), 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.

---

[8] Council of Europe. Convenio sobre la ciberdelincuencia (ETS No. 185). *Budapest*, 23.XI.2001. Recuperado de https://www.coe.int/en/web/cybercrime/the-budapest-convention

[9] Ratificaciones y adhesiones del Convenio de Budapest al 07 de marzo de 2024. Recuperado de: http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=TomHTOvO

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

En el Título 4, 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.

Por último, el Título 5 que lleva por nombre *"otras formas de responsabilidad y sanción",* establece ciertas disposiciones comunes para todos los delitos de la Sección 1, vinculadas a la tentativa y la participación criminal (art. 11 CB). También se determinan condiciones de responsabilidad para las personas jurídicas (art. 12 CB), y por último, a las sanciones y medidas aplicables, tanto a personas físicas como jurídicas (art. 13 CB).

Aclaramos en este punto que el convenio no determina escalas penales específicas de multas, inhabilitación o prisión. Solamente se indica el tipo de sanción aplicable para estos hechos, imponiendo en este marco que sean "incluidas" penas privativas de libertad para las personas físicas, y las sanciones pecuniarias para las jurídicas.

Según la normativa convencional, los Estados Parte se comprometen a limitar las sanciones que han consagrado y ejecutado en materia de ciberdelitos, debiendo ser las mismas efectivas, proporcionadas y disuasorias.

III.- LOS PROTOCOLOS ADICIONALES DEL CONVENIO DE BUDAPEST COMO REAFIRMACIÓN DE LOS COMPROMISOS INTERNACIONALES FRENTE A LA CIBERDELINCUENCIA

El primer protocolo adicional al Convenio de Budapest surge el 28 de enero de 2003, y tiene por misión dar respuesta a la necesidad de tipificación penal de actos racistas y xenófobos cometidos en sistemas informáticos (art. 1 1er PCB).

Aborda en este marco nuevas concepciones para abordar la problemática[11]. Además, hace suyas las definiciones abordadas en el Convenio de Budapest, que sean aplicables al protocolo (art. 2 1er PCB). Una vez definida la finalidad y conceptos elementales, se establecen las exigencias legislativas de carácter penal a los países signatarios: a). Difusión de material racista y xenófobo mediante sistemas informáticos (art. 3 1er PCB). Con posibilidad de reserva condicionada; b) Amenazas con motivación racista y xenófoba, mediante sistemas informáticos (art. 4 1er PCB). Sin posibilidad de reserva; c) Insultos con motivación racista y xenófoba, mediante sistemas informáticos (art. 5 1er PCB).

Con posibilidad de reserva total o parcial; d) Negación, minimización burda, aprobación o justificación del genocidio o de crímenes de lesa humanidad (art. 6 1er PCB). Con posibilidad de reserva total o parcial. Aclara el protocolo que estos delitos deben ser

[11] El Protocolo (2003) define al "material racista o xenófobo" como todo material que "propugne, promueva o incite al odio, la discriminación o la violencia, contra cualquier persona o grupo de personas, por razón de la raza, el color, la ascendencia o el origen nacional o étnico, así como de la religión en la medida en que ésta se utilice como pretexto para cualquiera de esos factores" (p. 2).

"intencionales y sin derecho". Ello nos acerca a la idea de que los mismos no admitirían una modalidad típica imprudente.

El artículo 7 1er PCB consagra la exigencia legislativa de contemplar formas de participación criminal dolosa para los delitos enumerados en los párrafos anteriores.

El 12 de mayo de 2022, se conforma el Segundo Protocolo Adicional del Convenio de Budapest, el cual tiene por objetivo establecer nuevas medidas de cooperación internacional, condiciones de divulgación de pruebas electrónicas, y exigencias en materia de pesquisa para los delitos informáticos abordados por el CB y el 1er PCB.

IV.- RECEPCIÓN DEL CONVENIO Y SUS PROTOCOLOS ADICIONALES EN LA ARGENTINA.

Previamente, es saludable aclarar que, en nuestro país, una década antes de la aprobación de la Convención en trato, ya existía una ley de delitos informáticos Nº 26.388, que data del 2008. La aprobación local del Convenio de Budapest, tuvo lugar en nuestro país mediante ley 27.411 del 22 de noviembre de 2017 (con entrada en vigor 01 de octubre de 2018), estableciendo determinadas reservas que son coherentes, como veremos en el análisis posterior, con nuestro ordenamiento penal vigente.

Frente a la exigencia de incorporación de delitos informáticos al catálogo argentino, la Argentina hizo reserva del art. 6.1.b CB, que establece la necesidad de tipificar penalmente la posesión de dispositivos virtuales o físicos, como así también contraseñas o datos similares que permitan el acceso a un sistema informático, para cometer "intencionalmente" los delitos expresados en el Convenio (arts. 2 a 5 CB). Ello en razón de que, a criterio del Estado Parte, se anticipa con esta norma la punición para alcanzar actos preparatorios no pasibles de injerencia por imperativo constitucional (art. 19 CN).

También se hizo reserva de los arts. 9.1 d CB, que impone tipificar la adquisición para así o para terceros de pornografía infantil por sistemas informáticos. También se limita a nivel local el alcance que establece el convenio para la definición de "pornografía infantil", abarcando solamente casos de menores adoptando un comportamiento sexualmente explícito, y excluyendo los que tengan personas parecidas a menores o imágenes realistas con representaciones de menores (9.2.b y 9.2.c CB). Ello se debe (según veremos infra) a su incompatibilidad con la ley de delitos informáticos (ley 26.388).

En cuanto al art. 9.1.e, que establece la necesidad de prohibir la posesión de pornografía infantil en un sistema informático o en un dispositivo de almacenamiento de datos, también el Estado argentino hizo reserva parcial. Ello se debe a que, en la Argentina, este hecho ya se encuentra contemplado en el art. 128, segundo párrafo, del CPA, bajo ciertas condiciones vinculadas a la ultrafinalidad el autor tendiente a la trascendencia del material a terceros (fines inequívocos de distribución o comercialización).

Por último, haremos mención de las dos últimas reservas efectuadas, que no están vinculadas al código penal sino más bien a cuestiones de competencia procesal o de reglas internacionales de cooperación.

El Estado hace reserva del art. 22.1.d CB, que establece la posibilidad de invocar la competencia argentina para la investigación de hechos cometidos en el extranjero por sus nacionales. Ello se debe a que en nuestro país, el principio de nacionalidad activa solo puede invocarse si el autor que cometió el delito en el extranjero se encuentra en la Argentina al momento de su requisitoria, siempre que no haya un tratado de extradición que obligue la entrega de nacionales (art. 12 de la ley de cooperación internacional).

El art. 29.4 CB también fue pasible de reserva por la Argentina, en razón de que el Estado argentino, por su legislación vigente y los principios que son reconocidos allí en materia de cooperación internacional, no puede contribuir con países extranjeros en la investigación de hechos tipificados en el convenio si no tienen consagración expresa en nuestro país (principio de doble incriminación, art. 6 ley 24.767). La contribución en la normativa citada consiste en vistas a registros de datos del país requerido, revelación de datos almacenados y conservación de los mismos.

En cuanto a los protocolos adicionales, la Argentina no se adhirió en forma alguna al Primer Protocolo. Sin embargo, en relación al segundo protocolo adicional, el Estado argentino el 16 de febrero de 2023 expresó su voluntad de adherirse a su contenido mediante la suscripción al Convenio por parte de los representantes del Poder Ejecutivo Nacional, quedando pendiente el trámite legislativo para su aprobación, con las reservas que pudieran darse[12].

Dentro del marco de recepción expuesto, resulta imperioso efectuar el análisis de los ciberdelitos que surgen a nivel local con la ley 26.388, y verificar luego de ello el grado de acatamiento existente en nuestro país de las medidas legislativas de derecho penal sustantivo impuestas por el Convenio de Budapest, cuyo análisis dogmático lo plantearemos a continuación.

En cuanto a los protocolos adicionales, verificaremos si fueron incorporados a nuestra legislación local los tipos penales que aquellos establecen (concretamente el primer protocolo), a pesar de la falta de aprobación del instrumento internacional en nuestro país.

A modo de aclaración previa, por razones de extensión del presente artículo, no abordaremos las cuestiones vinculadas la evidencia digital, de competencia de los tribunales, de cooperación internacional o de otros problemas vinculados al derecho procesal.

---

[12] Council of Europe Oficial. Oficina de Tratados. Lista de tratados para un Estado específico https://www.coe.int/en/web/conventions/full-list?module=treaties-full-list-signature&CodePays=ARG

V.- LAS SIGNIFICACIONES INCORPORADAS AL ART. 77 DEL C.P. Y SU RELACIÓN CON LA TERMINOLOGÍA DEL CONVENIO DE BUDAPEST (ART. 1 CB)

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 (2008) en su artículo 1º incorpora el concepto de documento, adoptando un carácter más amplio en 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" (párr.2). 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 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 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 (2001) 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[13].

Habiendo expresado el nuevo alcance de las definiciones otorgadas 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. A tal fin, agruparemos las normas legales y convencionales en categorías, empleando el nombre de los cinco títulos establecidos en el Convenio de Budapest.

---

[13] La norma internacional define en su art. 1º: "… *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…"* (p. 4).

VI.- TÍTULO I CB: DELITOS CONTRA LA CONFIDENCIALIDAD, LA INTEGRIDAD Y LA DISPONIBILIDAD DE LOS DATOS Y LOS SISTEMAS INFORMÁTICOS

El Título I de la Sección I del CB se encarga de establecer obligaciones a los Estados signatarios de proteger penalmente determinadas modalidades de afectación a bienes jurídicos concretos, a saber: "...la confidencialidad, la integridad y la disponibilidad de los datos y los sistemas informáticos...".

Siguiendo esta exigencia, incluso antes de la aprobación local del CB (conforme lo analizado supra), ley Nº 26.388, artículo 3º, modificó la denominación del Capítulo III, ubicado en el Libro II (de los delitos), Título V del CP (delitos contra la libertad), por el de "Violación de Secretos y de la Privacidad", sustituyendo de una serie de tipos penales para abarcar toda forma de intrusión a datos secretos, componentes electrónicos ajenos y/o interceptación de comunicaciones (email, streaming, etc.), sin el consentimiento de su titular.

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.

También veremos que, en aras de proteger los bienes jurídicos indicados por el Título I del CB, la ley 26.388 se encarga además de establecer prohibiciones penales a la integridad y disponibilidad de datos, sistemas informáticos y comunicaciones en los Títulos VI (delitos contra la propiedad) y VII (delitos contra la seguridad pública).

VI.I.- DATOS Y SISTEMAS INFORMÁTICOS: ACCESO Y REVELACIÓN ILÍCITA

En cuanto al acceso ilícito, este fue incorporado al código penal mediante los art. 153 bis[14] y art. 157 bis del CP, inc. 1[15].

Estas previsiones buscan dar respuesta al CB (2001) en la punición del hacking intrusivo, el cual figura en el art. 2[16] del referido instrumento internacional.

---

[14] Expresa el texto legal: *"…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…"* (CP, 2008, Art. 5).

[15] Expresa el texto legal: *"…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…"* (CP, 2008, Art. 8).

[16] Expresa el texto convencional: *"…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…"* (p. 4).

El bien jurídico que busca proteger la ley penal es la privacidad en un sistema o dato informático (153 bis CP) o de un banco de datos (157 bis, inc. 1, CP) y los secretos que en su esfera privada se albergan. Para Palazzi (2018) la privacidad que se busca proteger puede ser tanto de una persona física como jurídica. Según Aboso (2020), se busca proteger penalmente la libertad de comunicación, de información y la intimidad "...esta última como el espacio en el cual la persona tiene garantizada de manera integral su derecho de ejercer un plan de vida determinado con exclusión de la injerencia arbitraria de terceros o del propio Estado..." (p. 143). Constituye en consecuencia, la decisión del titular del espacio o elemento virtual en cuestión, de decidir quién puede ingresar a aquel, en razón de la información sensible o personal que pudiera existir allí.

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 éste último establece. 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 ingeniería social mediante "phishing"[17], "SIM Swapping"[18], llamadas o mensajes telefónicos de falsos interlocutores (gobierno, empresas de servicios, bancos, etc.), hasta el uso malwares[19] que ingresan a los sistemas mediante descargas de software, de archivos, etc.

La jurisprudencia ha encuadrado en la figura del art. 153 bis del CP a ciertos casos donde la autorización para acceder expiró pero, sin embargo, se continuó actuando en ese sentido, generando serios perjuicios a sus víctimas. En la causa de la Cámara Federal de Casación Penal, caratulada "Ranieli, Germán Walter s/ violación sistema informático, art. 153 bis, 1° párrafo", Reg. No. 178/17, 30 de marzo de 2017, se buscó frente a la calificación atribuida interponer por defensa el apoderamiento de la dirección de IP del declarante por parte otra persona (siendo ésta última supuesta autora y no el condenado). El tribunal confirmó la condena de la instancia anterior, expresando entre sus argumentos que la cuestión del IP no resulta vinculante para condena, si no se la valora junto a otras pruebas que respalden el empleo de tal protocolo[20].

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

[18] Concepto de de SIM Swapping en 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/

[19] Concepto de Malware en *¿Que es el malware?* https://www.microsoft.com/es-ar/security/business/security-101/what-is-malware

[20] Fallo disponible en: https://www.cij.gov.ar/nota-25440-Casaci-n-Federal-ratific--condena-por-el-delito-de-acceso-ileg-timo-a-un-sistema-o-dato-inform-tico-restringido.html.

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, la doctrina entiende que tanto las conductas del art. 153 bis como del 157 bis, son dolosos, que exige dolo directo (Aboso, 2020).

Respecto de la autoría, el hecho puede ser cometido por cualquier persona. Respecto de la caracterización de estos hechos, los descriptos 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 (Palazzi, 2016).

Consideramos que existen una serie de artículos de la ley penal que se encuentran vinculados, los cuales hacen referencia a un exceso en la autorización para el acceso de datos, más que el acceso en sí. Entre ellos encontramos al art 157 del CP[21].

El bien jurídico al decir de Riquert (2016) 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..." (p. 3).

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 secreto. Donna (2011), haciendo referencia a Solsona, expresa que: "La acción no consiste en 'divulgar', sino en 'revelar' que, si bien va más allá de comunicar, no implica publicar" (p. 449).

En cuanto al tipo subjetivo, el delito es doloso de dolo directo (Aboso, 2020), 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, el 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, según el art. 157 bis, inc. 2[22], la revelación también puede alcanzar a bancos de datos personales, de acuerdo a nuestra ley penal.

---

[21] Expresa el texto legal: *"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."* (CP, 2008, art. 7).

[22] Expresa el texto legal: *"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"* (CP, 2008, art. 8).

El bien jurídico es la intimidad de los datos personales. Refiere Aboso (2020), siguiendo a Tazza/Carreras, que: "...El bien jurídico tutelado sigue siendo la intimidad de las personas, en especial, respecto de los datos personales almacenados en un sistema informático..." (p. 190).

Son dos las acciones típicas. 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) la conducta del inc. 2 sería admisible a título de dolo eventual. En cambio, para Donna (2011), no sería admisible el dolo eventual "debido a su redacción" (p. 453).

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 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.

Un fallo importante de la Cámara Nacional en lo Criminal y Correccional Federal, Sala II, es el que tiene por carátula "Karamanian, Sebastián y otros s/ procesamiento y pp", expte. CFP 12474/2017/44/CA5[23], fecha de la resolución 04 de abril de 2018, donde se trató la operatividad del art. 157 CP. Se confirmó el procesamiento de los imputados funcionarios de la AFIP, por filtración de datos del sinceramiento fiscal y posterior publicación en un diario Página 12, en relación a cinco contribuyentes pertenecientes al entorno de funcionarios gubernamentales[24]. Respecto a la posibilidad de aplicar la norma del art. 157 bis, la Cámara descartó esta posibilidad afirmando que: "...configuran violación de secretos en los términos del art. 157 del CP, tanto en el caso de los autores (funcionarios) como de los partícipes (particulares), pues se ha acreditado la revelación de datos que por ley debían permanecer en reserva...". Entendemos, conforme surge auto de apelación, que este descarte se debe a la fuente del dato secreto, que no constituyen "bancos de datos personales": remisiones de balances, datos vinculados a presentaciones fiscales, valuaciones fiscales de automóviles, etc.

---

[23] Fallo disponible en: https://www.cij.gov.ar/nota-29729-La-C-mara-Federal-confirm--procesamientos-en-la-causa-contra-funcionarios-de-AFIP-por-tr-fico-de-datos-fiscales-secretos.html

[24] En los términos del fallo: *"...Estos datos, por ley, son secretos y las razones son obvias: su sensibilidad, su carácter privado en la mayoría de los casos y las consecuencias negativas para los ciudadanos que puede implicar su difusión. Por todo ello, los funcionarios públicos que tienen acceso a las bases que los almacenan tienen una obligación normativa de mantener su reserva* (art. 101, ley 11683; art. 157 CP)..." (CNCCF, Sala II, "Karamanian, Sebastián y otros s/ procesamiento y pp", expte. CFP 12474/2017/44/CA5, fecha de la resolución 04 de abril de 2018).

VI.II.- COMUNICACIONES ELECTRÓNICAS: ACCESO INDEBIDO, APODERAMIENTO E INTERCEPTACIÓN ILÍCITA PARA SU DESVÍO O SUPRESIÓN.

El **art. 153 del CP**[25] refleja una respuesta del Estado argentino a las previsiones del **art. 3 del CB**[26], en la lucha por evitar toda interceptación malintencionada de comunicaciones entre usuarios.

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. Arocena (2012), siguiendo a Palazzi, expresa el concepto de comunicación electrónica como: "...debe entenderse todo mensaje enviado por un remitente a un destinatario, a través de un sistema electrónico...".

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, mediante una violación en los protocolos de seguridad o excediendo el ámbito de lo permitido (Aboso, 2020). 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 tal elemento ajeno para su disposición. En razón de la cualidad virtual de la comunicación, el autor del delito puede "clonar" la misma, sin que su dueño siquiera se enterara, pues la comunicación original seguirá sin alteraciones en el mismo lugar en el que se encontraba.

Una resolución que aborda el alcance de esta figura (quizás en forma escueta) es la emitida por la Cámara Nacional en lo Criminal y Correccional, Sala VII, en autos "M, M. s/ Violación de correspondencia" Expte 39.727. C 2/59, fecha de la decisión 21 de octubre

---

[25] Expresa el texto legal: *"…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…*" (CP, 2008, art. 4).

[26] Expresa el texto convencional: *"…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…"* (CB, 2001, p.3).

de 2010[27]. En ella se revocó un sobreseimiento (indicando que el caso encuadra en el art. 153 CP) respecto de una persona que ingresó a una casilla de correo electrónico ajeno con clave, para luego cambiar la misma y difundir el contenido de los mails de la víctima.

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) 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... (p. 27).

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…" (2013, p. 27).

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 grupo determinado de personas, en cambio, la idea de publicación implica una difusión a un número indeterminado de éstas. Coincidimos con Riquert (2013) al entender que "*comunicar*", quiere decir hacer conocer a un tercero que no participa del delito el contenido de la correspondencia. Según Aboso (2020) no existe acuerdo en doctrina respecto del requerimiento de identidad entre quien accede y quien comunica o publica[28], aclarando que esto cobra especial importancia en la pugna entre el derecho a la intimidad contra la libertad de prensa:

> ...Esta relación de tensión entre ambos derechos amparados constitucionalmente genera la necesidad de una valoración adecuada y

[27] Fallo disponible en: https://www.cij.gov.ar/nota-5530-Revocan-sobreseimiento-a-una-persona-que-viol--una-casilla-de-mail-y-difundi--su-contenido.html

[28] Según el autor citado, a favor: Soler, Fontan Balestra/Ledesma, entre otros. En contra: Creus/Buompadre.

> proporcional a los intereses en pugna. Cuando existen intereses públicos en juego, por ejemplo, casos de corrupción publica o privada, el derecho a la información y a la libertad de prensa adquieren una posición de preeminencia frente a los intereses particulares... (p. 160).

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, Palazzi (2016) indica que, según Soler y Nuñez, la expresión "indebidamente" señala la imposibilidad de actuar de forma culposa. Sin embargo, refiere que, siguiendo a Nuñez, el desvío o supresión admitiría únicamente la forma dolosa, con posibilidad de dolo eventual. Para Aboso (2020), al igual que con el art. 153 bis, son delitos dolosos que solo admiten dolo directo.

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. Según Aboso (2020), son delitos de mera actividad y de peligro abstracto.

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 tal orden, el **art. 155 CP**[29] establece la publicación abusiva de una comunicación electrónica no autorizada.

Como bien jurídico se considera 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, Telegram, etc.) que estuviera en poder del autor, causando perjuicio a terceros.

Respecto del tipo subjetivo, según Donna (2011) y Aboso (2020) 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, 2015, p. 4).

Autor sólo puede serlo quien es poseedor de la correspondencia no destinada a publicidad. Es un delito de resultado que admite la tentativa (Riquert, 2015). Para Aboso

---

[29] Expresa el texto legal: *"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"* (CP, 2008, art. 6).

(2020), en cambio, es un delito de peligro potencial o concreto pues, según el autor, no es necesario para su consumación el perjuicio económico.

Cabe agregar que el art. 155 CP, en un segundo párrafo, establece una excusa absolutoria, para quien haya tenido por fin con su acción evitar que se afecte un interés público: "...Está exento de responsabilidad penal el que hubiere obrado con el propósito inequívoco de proteger un interés público...". Para Arocena (2012), constituye una causa de justificación, en razón de la "...utilidad para todos los habitantes, ya del país todo, ya de una comunidad regionalmente determinada..." (p. 974).

Además de la normativa expuesta, es importante en este punto enunciar el **art. 197 del CP**[30]**,** el cual aborda la interrupción o entorpecimiento de una comunicación telefónica o telegráfica.

Este artículo no se encuentra comprendido en el Título V del CP, más allá de su relación con los artículos arriba analizados, y ello tiene que ver con el bien jurídico en juego, el cual pasa a ser colectivo (Titulo VII: Delitos contra la seguridad pública, Capítulo II: Delitos contra la seguridad del tránsito y de los medios de transporte y de comunicación).

El bien jurídico protegido por la norma en trato 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 (Palazzi, 2018).

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), 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) y admite la posibilidad de dolo eventual. Para Núñez (2008), 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. Indica Riquert (2018), que según Soler y Buompadre "...nos hallamos frente a una figura que requiere un resultado de lesión (interrupción, entorpecimiento o resistencia al restablecimiento) con el aditamento de un peligro para la seguridad común..." (p. 1723). Consideran (según el autor) que, de no llegar a verificarse el riesgo a grupos

[30] Expresa el texto legal: "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" (CP, 2008, art. 12)..

indeterminados, se podrá aplicar la tentativa. Por otro lado, expresa el profesor citado que, según Castelli y Barón de Astrada, estos delitos son de peligro abstracto, debido al riesgo estadístico que genera la conducta del autor a la seguridad común y por ende no admitiría tentativa.

VI.III.- ATAQUES A LA INTEGRIDAD DE LOS DATOS Y DEL SISTEMA

Las normas que *infra* se detallan, encuentran su vinculación con el Convenio de Budapest mediante el art. 4[31]. En primer lugar, analizaremos el **art. 157 bis, inc. 3,** del CPA[32].

El bien jurídico para Aboso (2020) es la intimidad de las personas "...en especial, respecto de los datos personales almacenados en un sistema informático..." (p. 190). Para Palazzi (2016) es la protección 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) 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 (p. 3).

Respecto del tipo subjetivo, se exige (en virtud de los elementos subjetivos y normativos que se incorporan: a sabiendas, ilegítimamente) el dolo directo. Aboso (2020) coincide, sin perjuicio de indicar que, según Donna, *"...se acepta dolo eventual..."* (p. 193).

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. En tal sentido, Palazzi (2016) considera que el resultado típico requiere una modificación del archivo, agregándose nuevos asientos o borrando los existentes.

---

[31] Expresa el texto convencional:*"…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…"* (CB, 2001, p. 4).

[32] Expresa el texto legal: "*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"* (CP, 2008, art. 8).

Por otro lado, **los arts. 183[33] y 184[34] del CP** establecen el daño informático.

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[35].

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 a 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*[36], 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

---

[33] Expresa el texto legal: "…*Será reprimido con prisión de quince días a un año …el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos…"* (CP, 2008, art. 10).

[34] Expresa el texto legal: *"…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…"* (CP, 2008, art. 11).

[35] Expresa el texto convencional: *"…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…"* (CB, 2001, p. 4).

[36] Concepto de Cracker informático en 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/

simplemente para divertirse. Así, mediante el "*ransomware*"[37], se han inutilizado sistemas enteros tornando imposible su recuperación debido al cifrado que se aplica en los mismos.

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 descriptas son dolosas (Palazzi, 2016). Macagno (2018), indica que:

> ...la voluntad de dañar la cosa, con conocimiento de los elementos del tipo objetivo -conocimiento de la ajenidad de la cosa y del carácter dañoso de la acción desarrollada- llevó a la mayoría de la doctrina a concluir en un dolo directo con exclusión...del dolo eventual... (p. 19).

Detecta el citado autor que en minoría, Soler y Damianovich de Cerredo abordan la posibilidad de dolo eventual "...dado que la letra de la disposición no autoriza a sostener sólo un dolo directo para la configuración del ilícito..." (p. 19).

Respecto de la autoría, cualquier persona puede ser autor, no se exigen condiciones especiales.

Cabe mencionar, que la jurisprudencia también ha valorado las características que debe poseer el autor para llevar adelante la maniobra prohibida. En tal sentido, la Cámara Federal de Casación Penal, Sala I, en autos "BORCHEZ AMIGO, FEDERICO s/ recurso de casación", Expte. CCC 62182/2016/2/CFC1, resolución del 12/10/2021, afirmó al momento de evaluar el encuadre típico de la figura en trato que, en razón del avance tecnológico y la falta de exigencia normativa respecto de sujetos activos concretos, no se exige para la comisión del delito analizado cualidades especiales[38].

Son delitos de resultado, toda vez que se da una transformación del elemento lógico, mediante las conductas descriptas *supra.* La tentativa es admisible. Aboso (2020) afirma en tal sentido que:

> ...será menester acreditar la relación de causalidad que debe mediar entre la acción típica y el resultado lesivo, es decir, debe comprobar en el caso concreto que le daño informático fue producto del uso de un acción del autor, por ejemplo, mediante el uso de un programa malicioso... (p. 362).

---

[37] Concepto de Ransomware en Ramírez H. (11 de agosto de 2021). Ransomware: Definición, tipos y tendencias 2021-2022. *Grupo Atico34*. Recuperado de: https://protecciondatos-lopd.com/empresas/ransomware/#Que_es_el_ransomware_Definicion

[38] Fallo disponible en: http://www.saij.gob.ar/camara-federal-casacion-penal-federal-ciudad-autonoma-buenos-aires-borchez-amigo-federico-recurso-casacion-fa21260324-2021-10-12/123456789-423-0621-2ots-eupmocsollaf?

La **segunda parte, 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[39].

El apartado de la normativa del 183 CPA toma como una conducta típica el "*vender*", consistente en realizar actos de comercio en 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 descriptas son dolosas. Indica Aboso (2020) que en general, la doctrina acepta el 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. Afirma Macagno (2018) que son delitos de peligrosidad abstracta "...sin necesidad de que se concrete el daño..." (p. 17). Consideramos que, en ciertos casos, la tentativa sería admisible. Imaginemos que, con el fin de introducir un programa malicioso en un sistema informático, el autor pone inserta un pendrive en una PC (bajo apariencia de un instalador inocuo), pero antes de descargarse el archivo en el disco rígido, el antivirus detecta el carácter peligroso del instalador e impide tanto la copia del archivo como su ejecución automática.

Volviendo al Convenio de Budapest, cabe aclarar dos cuestiones:

En primer lugar, la tenencia (como obtención) de programas informáticos con determinadas finalidades dañinas (para su utilización) que prevé el art. 6.1.a, no se encuentra alcanzado por el tipo legal del segundo párrafo del art. 183 CPA. Por ende, al no existir en nuestro país tipificación legal expresa para aquel acto de obtención, aquel acto previo a las conductas de disposición del material para causar daños a sistemas

---

[39] Expresa el texto convencional: *"…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…"* (CB, 2001, p. 4).

informáticos no sería punible. Abarcar a estos actos en el art. 183 importaría un avance del poder punitivo prohibido por imperio constitucional (atentaría el principio de legalidad, lex stricta, art. 18 CN).

Tampoco la norma toma como elementos prohibidos a los "dispositivos" (hardware), refiriéndose solamente a "programas" (software). Empero, a nuestro entender, la venta, distribución, circulación o introducción en sistemas informáticos de dispositivos sería igualmente punible, si dentro del dispositivo se encuentra albergado un programa destinado a causar daños (por ejemplo: el caso del instalador malicioso dentro del pendrive, que trabajamos supra).

En segundo lugar, conforme la reserva efectuada en la ley 27.411, la punición de toda posesión de elementos destinados a la comisión de delitos informáticos (6.1.b del CB) se encuentra vedada por decisión del Estado argentino. En relación a los motivos de esta reserva, observamos que el fundamento es muy escueto y superficial, sobre todo existiendo tipos penales de tenencia en nuestro sistema legal (para citar un ejemplo, el art. 14 de la ley 23.737 que regula la tenencia simple de estupefacientes).

VII.- TÍTULO II CB: LOS "DELITOS INFORMÁTICOS"

En este punto, revisaremos los puntos en común entre las previsiones del Título II de la Sección 1, Capítulo II del Convenio de Budapest y las normas de orden local que han acompañado tales imperativos internacionales.

A fin de evitar confusiones, es importante resaltar que con el título "delitos informáticos", el Convenio no busca negar "como delictivas" a las conductas analizadas en los puntos anteriores. Lo que se busca en el presente título es establecer la necesidad de proteger la faz "informática" o "virtual" de determinados bienes que ya contaban con protección penal, pero en entornos tradicionales o "físicos" (punto 79 del informe explicativo del Convenio de Budapest[40]). Sin embargo, hubiera sido positivo optar por un nombre que refleje de mejor manera esta exigencia para los Estados.

En el código penal argentino, según veremos *infra*, se da alcance legal a esta exigencia internacional de protección punitiva, mediante el Título XII (delitos contra la fe pública, Capítulo III: falsificación de documentos) y el Título VI (delitos contra la propiedad, Capítulo IV: Estafas y otras defraudaciones).

[40] Informe explicativo del Convenio sobre la Ciberdelincuencia, aprobado por el Comité de Ministros del Consejo de Europa en su 109ª reunión (8 de noviembre de 2001). Disponible en https://www.coe.int/documents/8475493/202017550/PREMS+015123+ESP+2023+Convention+Cybercrimininalite%CC%81+WEB+A5.pdf/a6b85c77-c79a-ef99-4d66-48351c1b48fc?t=1678890134243. p. 61.

VII.I.- 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. Esta decisión del legislador es coherente con lo indicado en el informe explicativo del CB.

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[41].

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 argentina, pues de la normativa del convenio, surge una finalidad requerida al autor, dirigida a buscar que se tengan por *"auténticos"* a los fines legales, aquellos "*datos*" que no lo son.

VII.II.- ESTAFA INFORMÁTICA

Los **incs. 15 y 16 del art. 173 del CP**[42] establecen formas de estafa por medios digitales. Estos artículos encuentran una relación con las previsiones del art. 8 del CB[43].

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.

---

[41] Expresa el texto convencional:*"…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..."* (CB, 2001, p. 5).

[42] Expresan los textos legales: *"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…"* (CP, 2004, Art. 1), "…*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."* (CP, 2008, art. 9).

[43] Expresa el texto convencional: *"…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…"* (CB, 2001, p. 5).

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) "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" (p. 78).

En cuanto a lo subjetivo, es un delito doloso de dolo directo (Riquert, 2018).

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. Afirma Arocena (2022), que el delito alcanza la consumación cuando se materializa la disposición patrimonial perjudicial.

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. La expresión defraudar en el contexto de la norma, busca establecer un tipo penal abierto, que no encuentre restricciones concretas para abarcar toda forma de abuso informático (Palazzi, 2016). 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.).

Un fallo donde se trató exactamente esta cuestión, es el emitido por la Sala VI de la Cámara Nacional de Apelaciones en lo Criminal y Correccional, en la causa Nro.39.779 "G. R. y otro s/ procesamientos", resolución del 03 de agosto de 2010. En aquel decisorio se confirmó el procesamiento de dos personas a raíz del uso de "*phishing*", mediante la creación de un portal paralelo de home banking, permitiéndoles obtener los datos necesarios para operaciones no autorizadas. Afirmó el tribunal que:

> ...En ese contexto, la circunstancia que el dinero de R. haya ingresado en la cuenta de G. al día siguiente de la obtención de los datos, mediante la

> manipulación informática (página paralela) denunciada (ver fs. 25, 28 y 34) es suficiente como para agravar la situación procesal de los indagados...[44].

En cuanto a lo subjetivo, es un delito doloso de dolo directo. Según Aboso (2022), la doctrina acepta la posibilidad de dolo eventual. Riquert (2018) expresa que: "...se ha explicado que en postura casi solitaria en el derecho nacional (pero, vale aclarar, no es de igual intensidad en el comparado), RIGHI y FERNÁNDEZ han sostenido la posibilidad de dolo eventual..." (p. 1492).

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 (Riquert, 2018). Consideramos que la transferencia bancaria efectuada por el transgresor en la cuenta de la víctima (y el consecuente vaciamiento parcial o total de la misma), ya consuma el delito. Ello en virtud de que, más allá de que el monto se mantiene en un ámbito virtual "pasible de retroacción", la víctima pierde el poder de disposición de las sumas de dinero sustraídas y el autor del delito gana poder de disposición de los fondos para emplearlos como quiera (pagar cuentas, comprar bienes, etc.), sin siquiera tener que extraer dinero del cajero automático (constituyen actos de agotamiento del delito). Claramente el bien jurídico propiedad fue lesionado.

Admite tentativa. Por ejemplo: El autor ingresa al *home banking* de la víctima y busca transferir fondos a otra cuenta. Sin embargo, no lo logra pues advierte la víctima haber sido víctima de un engaño y denuncia el hecho al banco antes de perfeccionarse la transferencia por el autor.

VIII.- TÍTULO III CB: DELITOS RELACIONADOS CON EL CONTENIDO

El ya mencionado informe explicativo del Convenio de Budapest, aborda en su punto 91 las razones de la elección del nombre indicado en el Título III: "delitos relacionados con el contenido". Allí surge que la elección se basó en el carácter del dato objeto del tráfico, consistente en archivos que contienen producciones audiovisuales (imágenes, audios, videos, y otra forma de representación) de pornografía infantil[45].

Nuestra ley penal sanciona estos hechos dentro del Título III (delitos contra la integridad sexual, Capítulo III).

---

[44] Fallo disponible en: https://www.cij.gov.ar/nota-4952-Confirman-el-procesamiento-de-dos-personas-por-fraude-informatico.html.

[45] Informe explicativo del Convenio sobre la Ciberdelincuencia, aprobado por el Comité de Ministros del Consejo de Europa en su 109ª reunión (8 de noviembre de 2001). Disponible en https://www.coe.int/documents/8475493/202017550/PREMS+015123+ESP+2023+Convention+Cybercrimininalite%CC%81+WEB+A5.pdf/a6b85c77-c79a-ef99-4d66-48351c1b48fc?t=1678890134243 . p. 64.

VIII.I.- PORNOGRAFÍA INFANTIL

El **art. 128 del CPA**[46] prohíbe una serie de conductas vinculadas a la pornografía infantil. Este artículo se vincula con el art. 9 del CB[47]. La normativa internacional, en complemento con el art. 1 CB, continúa ofreciendo definiciones en el art. 9 CB. En este caso, son específicas de la cuestión vinculada a los delitos de pornografía infantil en el ámbito virtual[48].

Es importante resaltar que, como lo adelantáramos *supra*, la ley local de aprobación del CB hizo reservas a este artículo[49]. En consecuencia, y de acuerdo a 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 reiteramos que, en razón de las reservas efectuadas en la ley de aprobación local al CB, solamente ingresaría en el concepto de pornografía infantil el material pornográfico vinculado a menores adoptando comportamientos sexualmente explícitos, no así cuando sean personas que parezcan menores o sean representaciones realistas de aquellos.

---

[46] Expresa el texto legal: *"…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…"* (CP, 2008, art. 2).

[47] Expresa el texto convencional: *"…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…"* (CB, 2001, p. 5).

[48] Expresa el texto convencional: *"…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…"* (CB, 2001, pp. 5/6).

[49] El art. 2 inc. b, de la ley 27.411 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…".*

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, salvo "…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 en forma expresa la mera tenencia dolosa de pornografía infantil al artículo 128 del CP. Por ende, a contramano de la reserva, 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.

En cuanto al bien jurídico protegido, expresa Aboso (2020) que la norma en cuestión abarca desde la producción hasta la distribución de material pornográfico:

> ...con la participación de menores de dieciocho años, razón por la cual no existen dudas que el interés jurídicamente protegido es el normal desarrollo sexual de las personas menores de esa edad desde la perspectiva de no ser expuestas a la explotación sexual por parte de terceros... (p. 207).

Expresa Dupuy (2017), que:

> ...el bien jurídico protegido, en las conductas de simple posesión, es la indemnidad sexual de los menores en general, como tipo de peligro...la posesión del material pornográfico infantil no protegería, de tipificarse, bienes personalísimos, sino la seguridad de la infancia en abstracto y su dignidad; pues el sujeto activo actuaría sobre un material ya elaborado... (p. 139).

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 Convenio de Budapest y la Convención sobre los Derechos del Niño, teniendo éste último jerarquía

constitucional en virtud de lo 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 la causa caratulada *"Tonnelier, Manuel S/Corrupción de Menor de 13 Años, Abuso Sexual - Art. 119 2° Párrafo y Publicaciones, Reprod. y/o Distrib. Obscenas"*, Expte. CCC 037537/2018/TO01, fecha de la sentencia 17/08/2021, el Tribunal Oral en lo Criminal y Correccional Nº 1 de la Capital Federal determinó en que consisten las representaciones sexuales explícitas, como así también la finalidad exigida por la norma penal en trato. En tal sentido, se indicó que los tocamientos y exhibiciones de genitales, practicas de sexo oral, tanto de menores (en el caso un menor de 9 años) como de mayores con participación de los primeros, importan este tipo de representaciones, sin existir finalidades diversas a las de la actividad sexual en sí (educativas, culturales, etc.)[50].

En cuanto al elemento subjetivo, son delitos dolosos. Consideramos que en todos los casos sólo puede admitirse el dolo directo (Aboso 2020). Riquert (2013) 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 a Riquert (2013), 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.

Según Aboso (2020), los delitos del primer y segundo párrafo del art. 128 CP, son delitos de pura actividad, que reflejan un peligro abstracto. Por ende, no admiten tentativa.

En el tercer párrafo del art. 128 CP, lo que interesa es que se tenga predominantemente la finalidad *distribución o comercialización* del material prohibido, caso contrario, de no probarse tal extremo (el cual debe ser inequívoca, como se ha afirmado *supra*), la conducta se desplazaría al segundo párrafo (relación de especialidad por ultrafinalidad). 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

[50] Fallo disponible en: https://www.cij.gov.ar/d/sentencia-SGU-c0848714-2c07-4489-ac50-b251ac37b94d.pdf

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 (Aboso, 2020).

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.

IX.- TÍTULO IV CB: DELITOS RELACIONADOS CON INFRACCIONES DE LA PROPIEDAD INTELECTUAL Y DE LOS DERECHOS AFINES

El presente título del Convenio contra la Ciberdelincuencia aborda la necesidad de protección penal de los derechos de autor, frente a afectaciones por medios virtuales. En este marco, el art. 10 del CB[51] establece estas exigencias para los países signatarios.

En nuestro país, la propiedad intelectual se encuentra protegida por la ley 11.723, incluyendo como objetos de protección datos o software (programas, sistemas operativos, obras audiovisuales, literarias, artísticas, científicas, etc.). Mediante el empleo y distribución no autorizado de los mismos a través de determinadas redes P2P, Torrent, clonación de datos de programas de streaming por software especial, etc., se afectan los derechos de sus autores, produciéndoles pérdidas increíbles en términos económicos a nivel global.

Con respecto al bien jurídico tutelado en los delitos de propiedad intelectual analizados en este apartado, seguimos el pensamiento de Gimbernat Ordeig (l992), afirmando que lo que se busca proteger es primordialmente el derecho de su titular o titulares de explotación económica de un bien inmaterial (obra artística, científica, etc.), y

[51] Expresa el texto convencional: *"…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…"* (CB, 2001, p. 6).

en segundo lugar "*...y esporádicamente...*", un derecho moral o personal del creador de la obra.

Compartimos estas reflexiones, pues solo de esta manera tiene un sentido claro del interés jurídico en la persecución de estos delitos.

Aparte, considerar merecedor de protección penal a un acto que no trasciende a terceros por presumir que su sola comisión importa "una ofensa a la moral del autor", dista de ajustarse a los límites impuestos por nuestra ley fundamental (art. 19 CN). Consideramos que ello no ocurre cuando se conecta la conducta en trato a actos posteriores, configurándose así actos que están dirigidos (como constitutivos de peligro, concreto o abstracto) a una lesión del bien jurídico (distribución y venta de la obra).

En otras palabras, el acto de "sacar fotos" de las páginas de un libro (reproducción) para un uso personal (por encontrarse la obra original en su poder en mal estado), muy difícilmente ofendería al titular de la obra. Por el contrario, se sentiría contento de saber que su libro se sigue leyendo a pesar de su antigüedad. Ello no es equivalente a la producción en serie mediante reimpresión de copias ilegales de libros con máquinas especiales para su posterior venta al exterior.

Estas cuestiones están estrechamente ligadas a la discusión actual en la ciencia penal, respecto de la legitimidad en la punición de los delitos de peligro abstracto, pudiendo citar a modo de ejemplo los delitos de estupefacientes (delitos de tenencia) o los de adulteración de moneda (falsificación), donde la regla de ofensividad juega un papel preponderante para la validez de tales tipos penales (en fallos de la CSJN: "Bazterrica"[52], "Arriola"[53], entre otros).

IX.I.- ESTAFA Y PROPIEDAD INTELECTUAL

La normativa local establece para la protección de los derechos intelectuales determinadas modalidades de afectación.

El art. 71 de la ley 11.723[54] reprime en los términos de la estafa genérica (art. 172 del CPA), a toda forma de defraudación de derechos de propiedad intelectual.

El art. 72[55], por su lado, efectúa una determinación concreta de las defraudaciones genéricas del art. 71, haciendo hincapié en determinadas modalidades.

---

[52] Fallo disponible en: http://www.saij.gob.ar/descarga-archivo?guid=rstuvwfa-llos-comp-uest-o86000507pdf&name=86000507.pdf

[53] Fallo disponible en: http://www.saij.gob.ar/descarga-archivo?guid=rstuvwfa-llos-comp-uest-o09000059pdf&name=09000059.pdf

[54] Expresa el texto legal: *"...Será reprimido con la pena establecida por el artículo 172 del Código Penal, el que de cualquier manera y en cualquier forma defraude los derechos de propiedad intelectual que reconoce esta ley..."* (ley 11.723, 1933, art. 71).

[55] Expresa el texto legal:*"...Sin perjuicio de la disposición general del artículo precedente, se consideran casos especiales de defraudación y sufrirán la pena que él establece, además del*

El verbo típico del art. 71 consiste en defraudar *"de cualquier manera y en cualquier forma"*, abarcando toda forma de afectación a los derechos de explotación sobre las obras, bajo modalidad de peligro o de lesión, no contenidos en los artículos que le son posteriores.

Emery (2009), expresa que es un tipo penal de carácter "abierto" (como toda violación de derechos autorales). En cuanto a sus características, afirma el autor, siguiendo a Anzorreguy, Da Rocha y Hernández Vieyra (1973) que: a) para su comisión se da pacíficamente, sin medios violentos; b) se da una desconexión entre la voluntad del transgresor y la del autor (no es necesario el contacto); c) inexistencia de desprendimiento físico debido a la incorporeidad del bien jurídico tutelado; d) falta de necesidad de desapoderamiento (se puede copiar sin despojar a la víctima del bien); e) entiende que puede no existir efectivo detrimento patrimonial. En este punto discrepamos, en razón de que los delitos de propiedad intelectual, cuando expresan conductas prohibidas que se muestran alejadas de otras pasibles de generar perjuicios patrimoniales al autor de la obra, necesariamente están conectadas en tanto son delitos de peligro en relación aquellos últimos, como parte de una progresión que puede o no tener lugar (por ejemplo: la reproducción en relación a la venta). Toda intervención del transgresor que no revele un peligro para el bien jurídico (incluso abstracto), carece de relevancia jurídico-penal por ausencia de ofensividad (art. 19 CN).

Respecto del art. 72 (como los demás delitos contra la propiedad intelectual), entendemos que existe una relación de especialidad con relación al artículo que le precede, y se determina un particular interés del legislador en la persecución y sanción de conductas concretas.

Los verbos típicos del inc. a son "*editar", "vender"* o *"reproducir"* obras inéditas "*sin autorización".* Según la doctrina, editar es una medio de reproducción de carácter impreso, escrito, material (Emery, 2009). Vender consiste en la comercialización de las obras a clientes determinados y/o indeterminados. Este último caso puede vincularse con la reproducción, el cual consiste en la realización "de uno o más ejemplares (copias) o de una parte sustancial de ella, en cualquier forma. (...) La violación del derecho de reproducción es la infracción por antonomasia contra la propiedad intelectual" (Emery, 2009, p. 292). Esta relación de conductas se advierte en, *"Causa n° 1552. Litman, Elías Daniel s/ infracción art. 72 de la ley 11723"*, donde la CSJN hizo lugar a un recurso de

secuestro de la edición ilícita: a) El que edite, venda o reproduzca por cualquier medio o instrumento, una obra inédita o publicada sin autorización de su autor o derechohabientes; b) El que falsifique obras intelectuales, entendiéndose como tal la edición de una obra ya editada, ostentando falsamente el nombre del editor autorizado al efecto; c) El que edite, venda o reproduzca una obra suprimiendo o cambiando el nombre del autor, el título de la misma o alterando dolosamente su texto; d) El que edite o reproduzca mayor número de los ejemplares debidamente autorizados..." (ley 11.723, 1933, art. 72).

queja por la querella, respecto de una absolución por la venta de fotocopias de un libro editado por Eudeba, a estudiantes universitarios, por un menor precio.

La *ausencia de autorización* indica la falta de consentimiento por parte del o los titulares de los derechos de explotación sobre la obra en trato. Dicha obra (elemento intelectual que recae sobre un soporte físico o virtual), debe ser *inédita o publicada*. Respecto de esto último, Emery (2009) expresa que con ello, la norma hace referencia a:

> ...cualquier obra, ya sea que el autor la haya mantenido en reserva o que la haya puesto a disposición del público...Para que exista infracción al derecho de reproducción, debe tratarse de la copia de una obra protegida o de una parte sustancial de ella... (p. 295).

Hay que diferenciar la protección en la reproducción, respecto del plagio. En el primer caso (reproducción) se exige para la protección la registración de la obra, y en el primer caso (plagio), al ser una arrogación de propiedad respecto del contenido de una obra ajena, no hace falta para su protección la registración (CNCom, Sala A, 5/2/96. LI., 1996-D-164, citado en Emery, 2009). Este último caso se encuadraría en las defraudaciones del art. 71 de la ley 11.723.

Entendemos que, para enmarcarlo en el mundo de los ciberdelitos, la frase *"por cualquier medio o instrumento"* abarcaría la edición, venta y producción de E-Books, archivos de imagen y/o audio y/o video, etc.

El inc. b establece como conducta típica la *falsificación* del nombre de la editorial que realmente se encargó de efectuar la edición. Estas conductas no solo afectan al autor, a la editorial, y toda persona con derecho a explotar las obras ya editadas, sino que hacen incurrir, según Ledesma (1992, 282), en un error al público adquiriente, haciéndoles creer que están comprando un texto que es legítimo, cuando es una impresión gráfica falsa.

El inc. c establece un acto de alteración del texto original (edición), su comercialización y reproducción, pero de una obra con sus datos esenciales e identificables (nombre del autor, título de la obra, o su texto) modificados o suprimidos. Cabe aclarar que, en este caso, no es necesaria la registración, ni tampoco que en forma anterior la obra haya sido editada por un equipo editorial o sello corporativo (como ocurre con el inc. a del art. 72), debiendo operar la protección desde su sola creación. Ello es así pues los derechos de explotación de la obra ya se encuentran en peligro con la edición, y muchas más con la reproducción y venta, más allá de que el autor decida mantener la obra en reserva. Esta postura que tomamos se condice con las discusiones arriba expuestas vinculadas al bien jurídico tutelado en estos delitos. En contra de nuestra postura, se encuentra Emery (2009), quien afirma que en este caso lo que se protege solamente es un derecho moral del autor.

Por último, el inc. d del art. 72 establece la prohibición penal de efectuar la edición y reproducción de un número de ejemplares por encima de los autorizados por el autor.

En otras palabras, el tipo penal sanciona todo exceso del editor, productor o empresario en la autorización oportunamente otorgada, afectando el patrimonio del creador de la obra literaria, musical, cinematográfica, etc. al no otorgarle las regalías que le son correspondientes.

En lo referente al tipo subjetivo, la doctrina entiende que estos delitos admiten la forma dolosa en todas sus formas, excluyendo la forma culposa (Emery, 2009).

El autor de estos delitos puede ser cualquier persona, no se establecen cualidades especiales, salvo en el caso del inc. d del art. 72 que exige (tácitamente) una cualidad de autor: un editor o reproductor previamente autorizado (delito especial propio).

Consideramos en este punto valioso de mencionar el caso "*Taringa!*" de la Cámara Nacional de Apelaciones en lo Criminal y Correcional, Sala VI, el cual (en realidad) lleva por carátula "Nakayama, Alberto s/ procesamiento", Causa N°42.318, resolución del 07 de octubre de 2011, donde se decidió confirmar el procesamiento de los dueños del portal de internet Taringa!, en razón de los links que se divulgaban allí, permitiendo así su reproducción ilícita. El tribunal entendió que se procedió a una participación criminal por facilitación. Ello en razón de que los usuarios, mediante la obtención de archivos con *copyright* desde el sitio, reproducían indebidamente obras con protección de derechos de autor[56].

Entendemos, siguiendo a Gimbernat Ordeig (1992), que son delitos de predominante actividad que tienen un resultado y que incluso admiten tentativa. El autor citado lo expresa de la siguiente manera:

> ...Los delitos contra la propiedad intelectual, incluso las modalidades que no exigen lesión efectiva de los derechos de explotación, se consuman con la producción de un resultado -algo que es común tanto a los delitos de actividad como a los de resultado- que no tiene porque coincidir espacio-temporalmente con la actividad previa desplegada... (p. 40).

Concretamente en relación a la tentativa, el profesor español afirmó lo siguiente: "...los ejemplares ilegales, no se producen simultáneamente, de ahí que estemos ante un delito de resultado y que, en consecuencia, sean concebibles tanto la tentativa como la frustración..." (p. 40).

IX.II.- REPRODUCCIÓN NO AUTORIZADA DE FONOGRAMAS

El art. 72 bis de la ley 11723[57] establece ciertas restricciones de carácter penal, concretamente para fonogramas (registros sonoros en soportes pasibles de reproducción),

---

[56] Fallo disponible en: https://www.cij.gov.ar/nota-8058-Confirman-procesamiento-de-responsables-del-sitio-de-Internet-Taringa--.html

[57] Expresa el texto legal: *"...Será reprimido con prisión de un mes a seis años: a) El que con fin de lucro reproduzca un fonograma sin autorización por escrito de su productor o del licenciado del*

frente a un uso comercial no autorizado de quienes tienen derecho de explotación sobre el mismo (productores o licenciados de productores).

Según se advierte de la transcripción efectuada, el inc. a del art. 72 bis establece como conducta típica *reproducir* el fonograma "*con fin de lucro"*, sin autorización escrita de quien sea productor o licenciado de productor. La doctrina entiende que la exigencia de autorización escrita es propia de la realidad comercial "...dado que para fabricar discos y casetes siempre se requiere el pedido de provisión, por escrito, del productor original o su licenciado..." (Emery 2009, p. 306).

El inc. b, por su lado sanciona penalmente las conductas de *facilitación* de reproducciones no autorizadas mediante *alquiler*. Consideramos que este artículo, por el avance tecnológico existente, no tendría razón de ser y por ello merece una reforma, pues los soportes materiales ya no se emplean desde la creación de las redes P2P para el tráfico ilícito de fonogramas mediante soporte virtual y no material (mp3, wav, etc.), perdiendo toda actualidad generar "un negocio" alquilando discos físicos. Muy difícilmente encontraremos hoy en día este tipo de comercios ilegales, pudiéndose en realidad encontrar actualmente tal facilitación, a nuestro parecer, en los entornos digitales.

Consideramos que una práctica ilícita similar podría emplearse mediante el "alquiler" de cuentas en plataformas digitales de streaming musical (Spotify, Apple Music, Deezer, etc.), abonando los clientes al titular sumas mensuales de dinero a cambio de las claves de acceso a tales espacios.

En el caso hipotético presentado, al titular de la cuenta se le otorga un usuario y clave intransferible pero, al compartirla con otros a título oneroso (por una mensualidad), dichas sumas de dinero no ingresan a la plataforma y mucho menos, a la cuenta bancaria del autor y quienes tengan derechos de explotación sobre el fonograma, perjudicándolos en este sentido.

---

productor; b) El que con el mismo fin facilite la reproducción ilícita mediante el alquiler de discos fonográficos u otros soportes materiales; c) El que reproduzca copias no autorizadas por encargo de terceros mediante un precio; d) El que almacene o exhiba copias ilícitas y no pueda acreditar su origen mediante la factura que lo vincule comercialmente con un productor legítimo; e) El que importe las copias ilegales con miras a su distribución al público. El damnificado podrá solicitar en jurisdicción comercial o penal el secuestro de las copias de fonogramas reproducidas ilícitamente y de los elementos de reproducción. El juez podrá ordenar esta medida de oficio, así como requerir caución suficiente al peticionario cuando estime que éste carezca de responsabilidad patrimonial. Cuando la medida precautoria haya sido solicitada por una sociedad autoral o de productores, cuya representatividad haya sido reconocida legalmente, no se requerirá caución. Si no se dedujera acción, denuncia o querella, dentro de los 15 días de haberse practicado el secuestro, la medida podrá dejarse sin efecto a petición del titular de las copias secuestradas, sin perjuicio de la responsabilidad que recaiga sobre el peticionante. A pedido del damnificado el juez ordenará el comiso de las copias que materialicen el ilícito, así como los elementos de reproducción. Las copias ilícitas serán destruidas y los equipos de reproducción subastados. A fin de acreditar que no utilizará los aparatos de reproducción para fines ilícitos, el comprador deberá acreditar su carácter de productor fonográfico o de licenciado de un productor. El producto de la subasta se destinará a acrecentar el "fondo de fomento a las artes" del Fondo Nacional del Derechos de Autor a que se refiere el artículo 6° del decreto-ley 1224/58..." (ley 23.741, 1989, art. 2).

Al no haber consagración expresa de estas conductas, consideramos las mismas serían pasibles de ingresar al art. 71 de la ley 11.723, que establece la defraudación genérica de derechos inmateriales para quienes tienen facultad de explotar económicamente la misma.

El inc. c establece la prohibición de *reproducir* copias de los fonogramas por precio y sin autorización. Considero que son pasibles las mismas críticas que las efectuadas para el inciso b del art. 72 bis, salvo por el importante hecho de que la norma, en este caso, no se limita a mencionar reproducciones únicamente materiales. Esto permitiría, por ejemplo, hacer responsable al autor de programas pagos destinados a "clonar" canciones (mediante grabación del sonido en alta calidad) en plataformas digitales de streaming musical. Actualmente sobran en la red programas que realizan estas actividades, permitiendo descargar en un formato offline (mp3, wav, etc.) música que está protegida por la plataforma de streaming.

El inciso d establece como conducta reprochable *almacenar o exhibir* las copias sin poder acreditar origen de tales fonogramas, mediante una factura de compra "comercial". Por otro lado, se sanciona con pena la *importación* de tales copias, estableciendo como ultrafinalidad el interés del transgresor en su distribución pública. Nuevamente, criticamos las normas mencionadas por no ajustarse a las nuevas exigencias de este siglo en materia de tráfico de fonogramas. En estos tiempos no encontraremos con facilidad un comercio que almacene y/o exhiba y/o importe copias de discos en soporte material pues, reiteramos, el avance de la tecnología hizo que la sociedad deje atrás los soportes físicos, para consumir música mediante *streaming*.

Al final del referido artículo se advierte el reconocimiento de facultades al o los damnificados para solicitar el secuestro y decomiso de los fonogramas materiales y de los dispositivos empleados para la reproducción, debiéndosele exigir al peticionante una caución judicial.

En lo referente al tipo subjetivo, se afirma que sólo adquieren relevancia penal en este aspecto, cuando exista dolo en la persona del transgresor, en todas sus modalidades (Emery, 2009).

El autor del delito puede ser cualquier persona, no se establecen cualidades especiales. Expresamos respecto al carácter del delito y la posibilidad de tentativa, que merecen las mismas observaciones que las efectuadas en el punto anterior (IX. I.).

IX.III.- REPRESENTACIÓN O EJECUCIÓN NO AUTORIZADA Y SUSPENSIÓN MEDIANTE ATRIBUCIÓN ILÍCITA DE DERECHOS

El art. 73 de la ley 11.723[58] otorga relevancia penal a conductas destinadas a la representación de obras para un público determinado (presentaciones en vivo o grabadas), respecto de obras teatrales, literarias, musicales, sin autorización de sus autores o derechohabientes.

Por su lado, el artículo 74[59] sanciona penalmente al falso titular de derechos intelectuales, cuando empleando tal calidad suspende representaciones o ejecuciones lícitas.

Las conductas del inc. a del art. 73 de la ley 11.723 consisten en *representar* o *hacer representar*. Esto se refiere a las personificaciones, expresiones corporales y verbales, que expresan ideas plasmadas en textos, en este caso de carácter teatral o literario (cuentos, novelas, etc.). Aquellas deben hacerse de manera pública y sin autorización del titular del derecho.

Las conductas del inc. b, por su lado, consisten en *ejecutar* o *hacer ejecutar,* también en forma pública y sin autorización, obras musicales. Es decir, que deben ejercerse actos de reproducción musical mediante el empleo de instrumentos, uso de la voz o con sonidos previamente grabados, en espacios de acceso a cualquier persona.

En ambos casos, a pesar de existir ejecución o representación, quedan fuera del tipo cuando estos tengan lugar en espacios domiciliarios o familiares (Emery, 2009). Entendemos que ello cambia cuando en un domicilio determinado se inician actividades de este estilo con fines de lucro con venta de entradas para ingresar al evento. También creemos que la norma en trato no niega la posibilidad de tipificar eventos "en vivo" o "grabados", en forma virtual mediante internet. Actualmente existen portales de "*streaming*" que permiten estas representaciones y ejecuciones. Por lo cual, al no exigir la norma que sean en lugares físicos públicos, nada obsta a extender la prohibición a los portales virtuales mencionados.

Por otro lado, las conductas del art. 74 consisten en *atribuirse* los derechos intelectuales, y a su vez (no de manera alternativa sino simultánea), *suspende* la representación o ejecución de una obra que no adolece de las características establecidas

---

[58] Expresa el texto legal: *"...Será reprimido con prisión de un mes a un año o con multa de MIL PESOS como mínimo y TREINTA MIL PESOS como máximo destinada al fondo de fomento creado por esta ley: a) El que representare o hiciere representar públicamente obras teatrales o literarias sin autorización de sus autores o derechohabientes; b) El que ejecutare o hiciere ejecutar públicamente obras musicales sin autorización de sus autores o derechohabientes."* (ley 11.723, 1933, art. 73).

[59] Expresa el texto legal: *"...Será reprimido con prisión de un mes a un año o multa de MIL PESOS como mínimo y TREINTA MIL PESOS como máximo destinada al fondo de fomento creado por esta Ley, el que atribuyéndose indebidamente la calidad de autor, derechohabiente o la representación de quien tuviere derecho, hiciere suspender una representación o ejecución pública lícita..."* (ley 11.723, 1933, art. 74).

en el art. 73. Según la RAE (edición 2001) suspender quiere decir *"...detener o diferir por algún tiempo una acción u obra..."*. No descartamos que estas suspensiones pueden darse también en entornos virtuales, realizando el transgresor una falsa denuncia de falta de autorización para mostrar una representación o ejecución en el portal de *streaming*, mediante datos apócrifos que busquen demostrar supuestos derechos intelectuales.

En cuanto al tipo subjetivo de las conductas expresadas en los arts. 73 y 74, nos remitimos a los puntos anteriores (pueden tener lugar las tres formas de dolo), bastando, como afirma la doctrina, que el transgresor haya actuado a pesar de haber no contar con el conocimiento efectivo (sino posible) respecto de la falta de autorización del titular del derecho de explotación de la obra (Emery, 2009).

El autor del delito puede ser cualquier persona, no se establecen cualidades especiales. Expresamos respecto al carácter del delito y la posibilidad de tentativa, que merecen las mismas observaciones efectuadas para el punto IX. I.

XIII.- DELITOS PENDIENTES DE TRATAMIENTO PENAL - 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 en 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.

En este año en el cual el Convenio de Budapest cumple veintitrés años desde su creación, podemos afirmar que existe una observancia casi total de sus previsiones en el orden interno argentino.

Sin embargo, nuestra legislación penal aún no aborda otras formas de intervención en el ciberespacio que indefectiblemente ponen en peligro o lesionan bienes que son sumamente valiosos, no solo para el individuo en su desenvolvimiento en internet, sino también para la sociedad en su conjunto o al Estado mismo, cuando mediante mecanismos informáticos comprometen su existencia.

En primer lugar, se considera como una misión pendiente de tratamiento punitivo los ciberataques a la infraestructura crítica del Estado. Estos consisten en el empleo de tecnologías en redes internas o de internet para afectar sistemas (tanto digitales como físicos) que (de acuerdo con el Anexo I de la Res. del Ministerio de Modernización del PEN Nº 1523/29):

> ...resultan indispensables para el adecuado funcionamiento de los servicios esenciales de la sociedad, la salud, la seguridad, la defensa, el bienestar social, la economía y el funcionamiento efectivo del Estado, cuya destrucción o perturbación, total o parcial, los afecte y/o impacte significativamente... (párr. 1).

Este tipo de perturbaciones las hemos visto en tiempos de pandemia, como también en espacios donde se llevan a cabo guerras. Así lo ha informado González (2022), en un artículo informativo para la firma ESET:

> ...Las organizaciones de todo el mundo deben mantenerse alerta ante la posibilidad de que se extiendan los ciberataques a medida que avanza el conflicto en Ucrania...los gobiernos deberían revisar los sistemas de defensa de los sectores críticos, ya que las consecuencias de un ciberataque a infraestructuras esenciales para la población puede tener consecuencias importantes... (parr. 1).

En nuestro país existe una clara preocupación por defender dicha infraestructura crítica frente a toda vulneración que pueda sufrir, existiendo una serie de normativas que buscan brindar definición y blindaje a estos ámbitos (determinación de requisitos mínimos de seguridad informática, implementación de programas seguros, comités y programas de protección, etc.)[60]. Sin embargo, a nivel penal no se han establecido prohibiciones frente a semejantes hechos.

En segundo lugar, podemos mencionar la sustitución o suplantación de identidad digital o "*phishing*". Se trata de una forma especial de fraude informático, consistente en hacer incurrir en error al usuario respecto de la identidad de un servicio, oficina gubernamental, comercio o empresa, o una persona, y obtener gracias a tal engaño datos confidenciales de cuentas bancarias, tarjetas de crédito, claves de acceso a portales y redes sociales, etc., para luego afectar el patrimonio, intimidad, o cualquier otro bien a sus víctimas[61]. Si bien existe la posibilidad de imputar estos hechos por el art. 173 inc. 16 del CP (cuando la propiedad se vea afectada), lo cierto es que el fin de la sustitución de identidad puede ser otro (afectar la intimidad, la dignidad, y hasta la integridad física), e incluso ser cometido el delito posterior por alguien que haya comprado la información confidencial y no por quien efectivamente ha obtenido la misma mediante estos mecanismos.

En tal sentido, han habido esfuerzos legislativos para determinarlo en forma autónoma en el catálogo de conductas prohibidas del CP, pero aún sin éxito.

Podemos mencionar el proyecto de incorporación del art. 139 ter sobre delito de suplantación o apoderamiento de identidad digital, presentada por la Diputada Carrizo el 27/06/2018[62]. También el proyecto "Borinsky" 2019, el cual en su Título Nº XXVI

---

[60] *Clasificación de estructuras críticas en Argentina*; disponible en: https://www.argentina.gob.ar/jefatura/innovacion-publica/direccion-nacional-ciberseguridad/normativa

[61] *Alcance del phishing en Argentina*; disponible en: https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/phishing

[62] Proyecto Carrizo (2018) disponible en: https://www.hcdn.gob.ar/diputados/mscarrizo/proyecto.html?exp=3868-D-2018

denominado "delitos informáticos", buscó darle consagración penal independiente a estas conductas, mediante su art. 491[63].

La llamada *"pornovenganza"* o "*revenge porn"* también ha sido pasible de trabajo legislativo en varios proyectos de ley. Este consiste en la difusión de imágenes o videos íntimos sin el consentimiento de quien o quienes aparezcan en ellas, en redes sociales, servicios de mensajería instantánea o cualquier tipo de medio social donde se comparte información[64].

El Título XXVI del proyecto "Borinsky" 2019, procuró trabajar el delito de pornovenganza en su art. 493[65], reconociendo agravantes[66]. Sin perjuicio de este proyecto de reforma estructural, actualmente se encuentra en trámite en el Congreso de la Nación la llamada "ley Belén" (proyecto 2757-D-22), la cual busca reformar las normas existentes para combatir estos hechos, como también los casos de "*deepfake*" (elaboración de imágenes o videos de índole sexual falsos empleando el rostro o cuerpo de la víctima)[67].

---

[63] Expresa el texto del proyecto Borinsky (2019): *"...Se impondrá prisión de SEIS (6) meses a DOS (2) años o SEIS (6) a VEINTICUATRO (24) días-multa, al que ilegítimamente con ánimo de lucro o la finalidad de cometer un delito, y valiéndose de alguna manipulación informática, ardid o engaño, obtuviere claves o datos personales, financieros o confidenciales de un tercero, siempre que el hecho no constituya un delito más severamente penado..."* (p. 483). Disponible en: http://www.bibliotecadigital.gob.ar/items/show/2572

[64] Concepto de *pornovenganza,* disponible en: https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/que-es-y-como-protegerse-de-la-pornovenganza#:~:text=Es%20la%20difusi%C3%B3n%20no%20consentida,pornovenganza%20un%20tipo%20de%20extorsi%C3%B3n.

[65] Expresa el texto del proyecto Borinsky (2019): *"...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...".* (p. 484). Disponible en: http://www.bibliotecadigital.gob.ar/items/show/2572

[66] Expresa el texto del proyecto Borinsky (2019): *"...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…"* (p. 484). Disponible en: http://www.bibliotecadigital.gob.ar/items/show/2572

[67] Expresa el texto del proyecto "Ley Belén" (2022):*"...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..."* (p. 1). Disponible en: https://www4.hcdn.gob.ar/dependencias/dsecretaria/Periodo2022/PDF2022/TP2022/2757-D-2022.pdf

El mencionado proyecto establece, además, que la acción penal para la persecución de estos delitos sea de oficio, dependiente de instancia privada.

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[68]. Por último establece la remoción digital de contenido que menoscabe la dignidad y la integridad de la mujer[69].

Otras conductas pendientes de ser tipificadas, son las de ciberocupación de dominios públicos o privados. Aquellas consisten en registrar un dominio de internet con un nombre ya existente, la cual corresponde a una empresa, institución o persona conocida, con el objeto generar engaño a los usuarios y lograr de esa forma afectar sus derechos[70].

En nuestro país se presentó un proyecto por los diputados Wechsler, Scaglia y Urroz (2017) a fin de modificar la ley de marcas y, en tal contexto actualizar la persecución penal para abarcar estos hechos[71]. Según la exposición de motivos del proyecto de reforma, se busca evitar todo menoscabo a los derechos de explotación en relación al nombre de una

---

[68] Expresa el texto legal:*"...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..."* (ley 27.736, 2023, art. 10).

[69] Expresa el texto legal: *"...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..."* (ley 27.736, 2023, art. 12).

[70] Concepto de ciberocupación disponible en: https://latam.kaspersky.com/resource-center/preemptive-safety/cybersquatting

[71] Expresa el proyecto Wechsler, Scaglia y Urroz (2017):*"...Modifícase el Artículo 31, Sección 1ª "Actos punibles y acciones", Capítulo III "De los ilícitos", de la Ley Nro. 22.362, que quedará redactado de la siguiente manera: Art. 31º.- Será reprimido con prisión de tres (3) meses a dos (2) años pudiendo aplicarse además una multa de pesos cuatro mil ($4.000) a pesos cien mil ($100.000) a: a) El que falsifique o imite fraudulentamente una marca registrada o una designación: b) El que use una marca registrada o una designación falsificada, fraudulentamente imitada o perteneciente a un tercero sin su autorización; c) El que ponga en venta o venda una marca registrada o una designación falsificada, fraudulentamente imitada o perteneciente a un tercero sin su autorización; d) El que comercialice productos o servicios con marca registrada falsificada o fraudulentamente imitada; e) El que usurpe el nombre de una marca registrada, a través de medios informáticos, con la intención de obtener un beneficio o causar un perjuicio, para sí o para terceros. El Poder Ejecutivo Nacional podrá actualizar el monto de la multa prevista, cuando las circunstancias así lo aconsejen..."* (párr. 1). Disponible en: https://www2.hcdn.gob.ar/proyectos/proyectoTP.jsp?exp=1591-D-2017

marca registrada por parte de usuarios malintencionados que busquen alcanzar un beneficio determinado o causar daño, abarcando los dominios de internet[72].

Claramente hay un vínculo entre estas acciones y las conductas de phishing, siendo las primeras un recurso para emprender actividades de clonación de portales web, y así lograr que la víctima introduzca datos privados en formularios "señuelo". Por tal motivo, encontramos en el art. 492 del Proyecto "Borinsky" de Código Penal (2019), un texto que integra estas dos conductas delictivas (suplantación de identidad y ciberocupación), cuando establece como conducta típica:

> ... al que a través de Internet, redes sociales, cualquier sistema informático o medio de comunicación, adoptare, creare, se apropiare o utilizare la identidad de una persona física o jurídica que no le pertenezca, con la intención de cometer un delito o causar un perjuicio a la persona cuya identidad se suplanta o a terceros... (p. 484)[73].

Las conductas de ciberodio no se encuentran específicamente tipificadas en el orden nacional (pero sí, como veremos, por vía interpretativa de las normas vigentes). Estas conductas expresamente son contempladas por el Primer Protocolo Adicional del Convenio de Budapest. Estas consisten, de acuerdo al referido instrumento internacional, en actos de índole racista y xenófobo cometidos mediante sistemas informáticos (art. 1 del Primer Protocolo del CB).

Sin embargo, cabe aclarar que ya existe una protección penal vigente para actos discriminatorios, mediante la ley 23.592. Esta establece determinadas sanciones penales, sin indicar expresamente el medio en que estas conductas pueden tener lugar[74].

Consideramos que se puede hacer una interpretación extensiva de estas conductas, cuando se empleen medios digitales para su comisión. Sin embargo, no descartamos la necesidad de que la normativa citada se actualice para hablar de discriminaciones de

---

[72] Expresa el proyecto Wechsler, Scaglia y Urroz (2017): "*...La acción de cybersquatting o su variante typosquatting en los nombres de dominio- técnica basada en los eventuales errores tipográficos en que puede incurrir un internauta a la hora de introducir en su navegador la URL de una página web- puede afectar a la identidad y reputación en Internet de una marca comercial. Un caso concreto de repercusión puede llegar a ser que el ocupador reproduce la imagen corporativa, diseño y contenidos del sitio original, creando un sitio web clonado que además tendrá un nombre de dominio muy parecido. El internauta puede llegar a interactuar con el sitio web falso, pensando que se trata del original...*". (párr. 6). Disponible en: https://www2.hcdn.gob.ar/proyectos/proyectoTP.jsp?exp=1591-D-2017

[73] Disponible en: http://www.bibliotecadigital.gob.ar/items/show/2572

[74] Expresa el texto legal:"*...Elévase en un tercio el mínimo y en un medio el máximo de la escala penal de todo delito reprimido por el Código Penal o Leyes complementarias cuando sea cometido por persecución u odio a una raza, religión o nacionalidad, o con el objeto de destruir en todo o en parte a un grupo nacional, étnico, racial o religioso. En ningún caso se podrá exceder del máximo legal de la especie de pena de que se trate. Art. 3°.- Serán reprimidos con prisión de un mes a tres años los que participaren en una organización o realizaren propaganda basados en ideas o teorías de superioridad de una raza o de un grupo de personas de determinada religión, origen étnico o color, que tengan por objeto la justificación o promoción de la discriminación racial o religiosa en cualquier forma. En igual pena incurrirán quienes por cualquier medio alentaren o incitaren a la persecución o el odio contra una persona o grupos de personas a causa de su raza, religión, nacionalidad o ideas políticas...*" (ley 23.592, 1988, art.2).

índole estructural (pues en la ley de 23.592 son abarcados en el concepto de actos discriminatorios en el art. 1, pero no en la norma penal del art. 2) y, además, mencionar expresamente los medios para cometer estos delitos (incluyendo los medios virtuales).

Por último, el proyecto "Borinsky" del 2019 aborda el llamado *"hurto informático"* en el art. 499[75]. Esta figura no existe actualmente en la ley penal vigente, ni tampoco en leyes especiales. Riquert (2018), en oportunidad de comentar los delitos informáticos contemplados por este proyecto de Código Penal, comparte las palabras de Carlos Christian Sueiro al expresar los antecedentes de esta normativa:

> ... ya en el año 1996 hubo proyectos de ley de los diputados Carlos R. Álvarez y José A. Romero Feris para tipificar el apoderamiento ilegítimo de bienes intangibles (datos, documentos, programas y sistemas informáticos). De allí que, sin dejar de reconocer la resistencia de un sector importante de la doctrina, se preguntaba por el olvido de este tipo en la reforma al CP concretada por la Ley 26388 del año 2008... (p. 15).

El referido autor, a su vez, señala un dato de no menor importancia en cuanto a los actos penalmente relevantes explicitados por la norma del art. 499 del proyecto de Código Penal aquí tratado, resaltando la importancia de considerar como conducta alternativa al apoderamiento, el "copiado" de información.

Ello resulta evidente en estos tiempos que transitamos, donde la tecnología avanza a niveles estrepitosos, permitiendo mayores facilidades para "clonar" los archivos o sistemas ajenos al menor tiempo posible, dado de carácter intangible de los objetos en cuestión y de los dispositivos que donde se almacenan.

Otra novedad que debe ser mencionada este 2024, es la que nos ofrece la Resol. del Ministerio de Justicia de la Nación Nº 25/2024, de fecha 28/02/2024, la cual ordena la creación de una nueva comisión para un anteproyecto de código penal, siendo liderada por el Cuneo Libarona, Buompadre, entre otros juristas. Confiamos en que allí se continuará con la empresa que los últimos proyectos intentaron sin éxito, tendiente a la protección penal integral al usuario y la sociedad en el mundo digital.

Sin lugar a dudas, 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 más tratados y convenios multilaterales.

---

[75] Expresa el texto del proyecto Borinsky (2019):*"...Se impondrá prisión de UN (1) mes a DOS (2) años, al que, violando medidas de seguridad, ilegítimamente se apoderare o copiare información contenida en dispositivos o sistemas informáticos ajenos que no esté disponible públicamente y que tengan valor comercial para su titular o para terceros..."*. (p. 485). Disponible en: http://www.bibliotecadigital.gob.ar/items/show/2572

Una de las medidas impuestas por el CB a la Argentina, más allá de los tipos penales o de las herramientas procesales que ofrece, tuvo recepción por resolución Nº 1291/2019, la cual establece que en el seno del Ministerio de Justicia y Derechos Humanos debe existir un contacto localizable 24/7 para la asistencia inmediata en la investigación penal de hechos cometidos a través de sistemas y datos informáticos o en la recolección de pruebas electrónicas. Todo ello en cumplimiento del art. 35 del CB.

No es una tarea sencilla, pero sin lugar a dudas la Argentina ha dado grandes pasos 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 (p. 01)[76].

BIBLIOGRAFÍA

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

Aboso, G. E. (2020). *Derecho penal cibernético: la cibercriminalidad y el Derecho Penal en la moderna sociedad de la información y la tecnología de la comunicación*. Editorial B de F.

Aboso, G. E. (2022). Ciberdelitos: análisis doctrinario y jurisprudencial. ElDial.com.

Arocena, G. A. (2012). La regulación de los delitos informáticos en el Código Penal argentino: Introducción a la Ley Nacional núm. 26.388. Instituto de Investigaciones Jurídicas de la UNAM. *Boletín Mexicano de Derecho, 45*(135), 945-988. Recuperado de https://dialnet.unirioja.es/servlet/articulo?codigo=4523885

Carnevale, C. A. (2008). *¿Es posible ser condenado penalmente por descargar música de internet? – Mp3, P2P, y garantías constitucionales.* Eldial.com.

Donna, E. (2011). *Derecho Penal – Parte Especial. Tomo II-A* (2º ed.). Rubinzal-Culzoni Editores.

[76] Frase citada por Ballesteros C. (2015) en el artículo titulado "la metamorfosis del cibercrimen". *El País.* Recuperado de: http://internacional.elpais.com/internacional/2015/04/16/actualidad/1429210295_215966.html.

Donna, E. (2011). *Derecho Penal – Parte Especial. Tomo II-C* (2º ed.). Rubinzal-Culzoni Editores.

Dupuy D., Kiefer M. (2017), *Cibercrimen I.* Editorial B de F.

Dupuy D., Kiefer M. (2018), *Cibercrimen II.* Editorial B de F.

Dupuy D., Kiefer M. (2020), *Cibercrimen III.* Editorial B de F.

Emery, M. A. (2009). *Propiedad intelectual: ley 11.723. Comentada, anotada y concordada con los tratados internacionales*. Editorial Astrea.

Gimbernat Ordeig, E. (1992). Otra vez: los delitos contra la propiedad intelectual. (Al mismo tiempo, algunas reflexiones sobre los delitos con objeto plural inequívocamente ilícito, sobre los de actividad y sobre el ámbito de aplicación de los artículos 13 y 15 del Código Penal). *Estudios Penales y Criminológicos, 15, 99-123*. Cursos e Congresos nº 71 Servizo de Publicacións da Universidade de Santiago de Compostela. Recuperado de: https://minerva.usc.es/xmlui/handle/10347/319/recent-submissions?offset=5

Gutiérrez R., Radesca L. C. y Riquert M. A. (2013). Violación de secretos y de la privacidad. *Revista Pensamiento Penal.* Recuperado de: https://www.pensamientopenal.com.ar/cpcomentado/37762-art-153-violacion-secretos-y-privacidad

Hertler, F. E. (2021). Ley penal y pedofilia en la red: pornografía infantil y child grooming en Argentina. *Conexiones, 1*(6), 150-171. Recuperado a partir de http://ojs.ucp.edu.ar/index.php/conexiones/article/view/790

Ledesma J. C. (1992). *Derecho penal intelectual: obras y producciones literarias, artísticas y científicas.* Editorial Universidad.

Macagno, M. E. (2018). Los daños simples y agravados. *Revista Pensamiento Penal.*https://www.pensamientopenal.com.ar/system/files/comentadas/comentadas46857.pdf

Núñez, R. (2008). *Manual de derecho penal, parte especial* (3º ed.). Lerner.

Palazzi, P. A. (2016). *Los delitos informáticos en el Código Penal*. Editorial Abeledo Perrot.

Riquert, M. A. (2013). Publicación ilegal de comunicaciones con otro destino. *Revista Pensamiento Penal.* https://www.pensamientopenal.com.ar/system/files/art.155_publicacion_indebida_de_correspondencia.pdf

Riquert, M. A.; Riquert, F. L. (2013). Art. 128: Difusión de Imágenes y espectáculos pornográficos de menores. *Revista Pensamiento Penal.*

https://www.pensamientopenal.com.ar/cpcomentado/37753-art-128-difusion-imagenes-y-espectaculos-pornograficos-menores

Riquert, M. A. (2014). Acceso ilegítimo a banco de datos personales, revelación ilegítima de su información e inserción ilegítima de datos. *Revista Pensamiento Penal*. https://www.pensamientopenal.com.ar/cpcomentado/40204-art-157-bis-violacion-datos-personales

Riquert, M. A (2015). Publicación ilegal de comunicaciones con otro destino. *Revista Pensamiento Penal.* https://www.pensamientopenal.com.ar/cpcomentado/42652-art-155-publicacion-indebida-correspondencia

Riquert, M. A. (2016). Revelación de hechos, actuaciones, documentos y datos secretos. *Revista Pensamiento Penal*. https://www.pensamientopenal.com.ar/cpcomentado/42933-art-157-revelacion-hechos-actuaciones-documentos-y-datos-secretos

Riquert, M. A. (2018). *Delitos informáticos en el anteproyecto de código penal de 2018*. https://riquertdelincuenciainformatica.blogspot.com/

Rubio, J. H. (2019). Internet y postmodernidad: un soporte de comunicación tan necesario como irreverente en la actualidad. Necesidades pedagógicas. *Vivat Academia*, *12*(146), 21-41. https://doi.org/10.15178/va.2019.146.21-41

NORMAS CITADAS

Council of Europe. Convenio sobre la ciberdelincuencia (ETS No. 185). Budapest, 23.XI.2001.

Informe explicativo del Convenio sobre la Ciberdelincuencia, aprobado por el Comité de Ministros del Consejo de Europa en su 109ª reunión (8 de noviembre de 2001).

Council of Europe. Primer Protocolo adicional al Convenio sobre la ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos (ETS No. 189). Estrasburgo, 28.I.2003.

Council of Europe. Segundo Protocolo adicional al Convenio sobre la Ciberdelincuencia, relativo a la cooperación reforzada y la divulgación de pruebas electrónicas (CETS No.224). Estrasburgo, 12.V. 2022

Ley 11.179, 30 de abril de 1922, Código Penal de la Nación Argentina.

Ley 26.388, 24 de junio de 2008, modificación del Código Penal. Boletín Oficial Nº 31433

Ley 27.411, 15 de diciembre de 2017, aprobación del Convenio sobre Ciberdelito. Boletín Oficial Nº 97934

Ley 11.723, 26 de septiembre de 1933, Régimen legal de la propiedad intelectual.

Ley 23.741, 18 de octubre de 2008, modificación a la ley Nº 11723.

Ley 25.930, 17 de septiembre de 2004, incorporación al artículo 173 de un inciso sobre defraudación mediante el uso de tarjetas de compra, crédito o débito. Sustitución del artículo 285. Equiparación a la moneda nacional de moneda extranjera y otros valores. Derogación del artículo 286.

Ley 27.736, 23 de octubre de 2023, Ley Olimpia, Ley Nº 26.485, Modificación. Boletín Oficial Nº 85200.

Proyecto Wechsler, Scaglia y Urroz (11 de abril de 2017). Marcas y designaciones - ley 22362 - modificación del articulo 31, sobre calumnia digital. Expediente 1591-D-2017. Publicado en: Trámite Parlamentario N° 27.

Proyecto Borinsky (26 de marzo 2019). Mensaje n° 60/19 y proyecto de ley de reforma al Código Penal de la Nación. Expediente PE-52/2019.

Proyecto “Ley Belén” (03 de junio de 2022). Código Penal de la Nación. Modificaciones penas para el delito de extorsión y la difusión no consentida de material íntimo, de desnudez y/o de material que retrata violencia sexual. Expediente Diputados: 2757-D-2022. Publicado en: Trámite Parlamentario N° 69.