REVISTA CHILENA DE DERECHO Y CIENCIA POLÍTICA
DICIEMBRE 2020 • E-ISSN 0719-2150 • VOL. 11 • Nº 2. PÁGS 122-144
RECIBIDO 06/08/2020 - APROBADO 15/12/2020
DOI 10.7770/RCHDCP-V11N2-ART2289

ARTÍCULO DE INVESTIGACIÓN

Delitos informáticos en el Código penal argentino

Computer-related crimes in the Argentine Criminal Code

María Belén Linares[1]
Universidad Católica Argentina (UCA), Argentina

RESUMEN La evolución de la Tecnología de la Información y la Comunicación (TIC) ha propiciado el nacimiento de un contexto criminógeno y, con ello, la incorporación de nuevos tipos penales. Este trabajo se propone analizar los tipos penales regulados en el Código penal argentino que se cometen mediante el uso de TIC. Estos tipos penales son producción, distribución y tenencia de pornografía infantil; ciberacoso sexual de menores; violación de correspondencia digital; acceso ilegítimo a datos o a sistema informático; publicación ilegal o abusiva de comunicación electrónica; revelación de secretos oficiales; acceso ilegítimo, difusión o alteración de datos personales; estafa o fraude informático; daño en datos y sistemas informáticos; interrupción o entorpecimiento de comunicaciones electrónicas; y alteración de medios probatorios.

PALABRAS CLAVE Tecnología de la Información y la Comunicación; delitos informáticos; Código penal argentino.

ABSTRACT The evolution of information and communications technology (ICT) has led to the emergence of a new criminogenic context, and with it, the incorporation of new types of crimes. The object of this paper is to analyse the criminal offences regulated by the Argentine Criminal Code that are committed using ICTs. These criminal offences are the production, distribution and possession of child pornography; cyber-bullying of children; violation of digital correspondence; unlawful access to data or to the computer system; illegal or abusive publication of electronic communications; disclosure of official

1. Doctora en Derecho por la Universidad de Sevilla (España), Licenciada en Derecho por la Universidad de Sevilla (España), Experta Universitaria en Victimología por la Universidad de Sevilla (España), Especialista en Derecho Penal por la Universidad de Belgrano (Argentina) y Abogada por la Universidad de Belgrano (Argentina). Profesora en la Universidad Católica Argentina (UCA). Mail: mblinares@hotmail.com.

secrets; unlawful access to, dissemination or alteration of personal data; computer fraud or embezzlement; damage to data and computer systems; interruption or obstruction of electronic communications; and alteration of evidence.

KEYWORDS Information and communications technology; computer-related crimes; Argentine criminal code.

I. Introducción

En los tiempos que corren al momento de redactar este trabajo, con la suave etiqueta del "aislamiento social preventivo obligatorio", la vieja "cuarentena" se ha reinstalado y nuestras prácticas habituales se han visto obligadas a una drástica y repentina reconfiguración. En este escenario, las modernas Tecnologías de la Información y Comunicación (en adelante, TIC) hacen más soportable el encierro, y es por ello natural el incremento sustancial de su empleo, mas también lo es su incidencia como factor criminógeno.

Hace ya tiempo que las nuevas tecnologías han adquirido un rol protagónico en la vida cotidiana, pero a la vez se han convertido en una herramienta que ha dado nacimiento a un ambiente propicio para la aparición de técnicas modernas y cada vez más sofisticadas de criminalidad. TIC ha supuesto, en algunas ocasiones, un condicionante para la comisión de clásicos delitos, mientras que, otras veces, ha conducido a la incorporación de tipos penales que hasta su aparición en el ordenamiento jurídico eran inexistentes o desconocidos para la sociedad y el legislador.

Este trabajo no pretende más que repasar precisos confines típicos de las figuras legales que regulan los hechos ilícitos que utilizan TIC para su comisión, incorporadas por el legislador en el Código penal argentino. Advertimos, desde ahora, que la mayor parte de esas figuras es resultado de la reforma experimentada por el ordenamiento de fondo con la Ley 26.388, no en vano conocida como la "ley de delitos informáticos"[2].

2. SUERIO (2018) apartado II. El autor dice textualmente: "*Hace tan sólo una década atrás la República Argentina adoptaba su primera ley destinada a la reforma integral en materia de criminalidad informática al Código Penal de la Nación. Nos referimos a la Ley 26.388. La ley 26.388 partió de una ley de reforma integral y concordada al Código Penal de la Nación basándose en el modelo de Proyecto de Ley de la Diputada Leonor Esther Tolomeo (1996) y llevó adelante la modificación de tipos penales tradicionales que la doctrina venían debatiendo durante más de dos décadas (1996-2008) y que se hacían presentes en cada uno de los proyectos de ley que se presentaron durante los doce (12) años previos*".

Entremos, pues, sin más demora, en la materia de estudio, para lo cual hemos adoptado un esquema que respeta la técnica legislativa vigente en el ordenamiento jurídico-penal argentino. Es decir, analizaremos, en este orden, las siguientes disposiciones que se ocupan de regular los delitos informáticos: arts. 128, 131, 153, 153 bis, 155, 157, 157 bis, 173 inc. 16, 183, 184, 197 y 255 del Código penal.

II. Delitos informáticos en el Código penal argentino

1. Producción, distribución y tenencia de pornografía infantil (art. 128 CP)

El texto del artículo 128 introducido por la ley 25.087, de 14 de abril de 1999, reflejaba la finalidad de proteger integralmente a la persona menor de 18 años como sujeto pasivo del delito, mediante el castigo penal de la difusión de imágenes pornográficas o espectáculos de dicha naturaleza, pero acotado a un ámbito de explotación individual[3]. Fue justamente esa restricción en su alcance, el motivo que suscitó numerosas críticas, pues el legislador penal con la otrora regulación no se refería, por ejemplo, a explotaciones colectivas o de criminalidad organizada, circunstancia esta última de alcance internacional[4].

La ley 26.388, de 24 de junio de 2008, y la ley 27.436, de 21 de marzo de 2018, sustituyeron sensiblemente el artículo 128 del Código penal argentino. La reforma de 2008, puntualmente, trajo consigo una modificación respecto de la anterior regulación del tipo penal, bastante más escueta y menos precisa, que solo castigaba la producción, publicación o distribución de imágenes pornográficas donde se exhibieran menores de 18 años. La ley 27.436, por su parte, llevó a cabo las siguientes modificaciones: *i*, en el primer párrafo, incrementó la escala penal; *ii*, en el segundo párrafo, dispuso el castigo penal a la simple tenencia de material pornográfico; *iii*, en el tercer párrafo, contempló una pena de seis meses a dos años para el que tuviere en su poder material pornográfico con fines inequívocos de distribución o comercialización; y, *iv*, en el último párrafo, incrementó la escala penal cuando la víctima fuera menor de 13 años[5].

3. Art. 128, del Código Penal argentino, conforme a la Ley 26.388, de 2008: "*Será reprimido con prisión de seis (6) meses a cuatro (4) años el que produjere, financiare, ofreciere, comerciare, publicare, facilitare, divulgare o distribuyere, por cualquier medio, toda representación de un menor de dieciocho (18) años dedicado a actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales, al igual que el que organizare espectáculos en vivo de representaciones sexuales explícitas en que participaren dichos menores. Será reprimido con prisión de cuatro (4) meses a dos (2) años el que tuviere en su poder representaciones de las descriptas en el párrafo anterior con fines inequívocos de distribución o comercialización. Será reprimido con prisión de un (1) mes a tres (3) años el que facilitare el acceso a espectáculos pornográficos o suministrare material pornográfico a menores de catorce (14) años".*

4. FIGARI (2018) p. 1.

5. Sobre la propuesta de tipificación en el proyecto de Código penal argentino de 2019, véase RIQUERT (2020) apdo. 3.

El primer párrafo del artículo 128 del Código penal quedó redactado del siguiente modo: "*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*".

Las acciones típicas consisten en producir, financiar, ofrecer, comerciar, publicar, facilitar, divulgar o distribuir, por cualquier medio, imágenes de pornografía infantil, entendiendo por tales, toda representación de un menor de 18 años dedicado a actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales[6]. La última parte del texto, que se refiere a la organización de espectáculos, podría haber configurado un párrafo separado, pues no guarda relación con los verbos típicos que le preceden al no vincularse con una actividad en vivo y en directo[7].

Los verbos típicos empleados por la figura permiten diferenciar dos grupos de acciones: uno, actos concretos de divulgación de pornografía infantil (como ofrecer, comerciar, publicar, divulgar o distribuir) y, otro, actos secundarios de ayuda para cometer el tipo penal, siendo en los hechos una suerte de actos de participación. Este catálogo de acciones se coronó con la expresión "por cualquier medio", que indica que la red informática puede configurar uno de cualquier otro medio de comisión de este delito[8].

La acción central de la figura consiste en "distribuir" imágenes pornográficas de menores de edad, que implica enviar a terceros la imagen[9] y que se caracteriza por su distribución en un número determinado de consumidores de ese producto, donde el

6. La Senadora Vilma Ibarra expresó, en la 18° Reunión, 14° *Sesión ordinaria, de 28 de noviembre de 2007, en el marco del debate parlamentario de la ley 26.388: "En materia de delitos contra la integridad sexual, en el actual artículo 128 sustituimos el concepto de 'imágenes pornográficas' por el de 'toda representación de un menor de 18 años dedicado a actividades sexuales explícitas' o 'toda representación de sus partes genitales con fines predominantemente sexuales,' tomando la definición del Protocolo Facultativo de la Convención sobre los Derechos del Niño relativo a la venta de niños, prostitución infantil y utilización de niños en pornografía. Conservamos -no entendimos por qué en Diputados se lo había quitado; pensamos que fue un mero error- la penalización de la conducta del que organizare espectáculos en vivo con escenas pornográficas en que participaren menores. Nosotros decidimos que era valioso mantener la punición de esta conducta que hoy está en nuestro Código Penal; así que la conservamos*".

7. RIQUERT (dir.) (2018b) p. 827.

8. LUCERO y KOHEN (2015) p. 49.

9. Consúltese, al respecto, sentencia dictada por la Sala I de la Cámara Nacional de Casación Penal en el marco del caso *Malomo, Enrique* (2013), que sirve de base para sostener que el envío a un solo correo electrónico podría constituir distribución si esta cuenta es una lista de distribución en

agente tiene cierto dominio sobre la cantidad de destinatarios. No resulta necesario para su tipificación que los destinatarios hayan, a su vez, accedido al material en cuestión. En cambio, la acción típica de "divulgar" no trae consigo la limitación en cuanto al número de destinatarios y, en consecuencia, el agente que divulga en los términos previstos por el tipo penal, no tiene control de la cantidad de destinatarios ni de la identidad de los mismos[10].

La acción de "producir" configura el verbo con mayor alcance. En este sentido, se ha dicho que "(i)*mplica el acto de la toma de fotografías o de imágenes en movimiento, de modo que, bajo nuestro derecho, la captación no autorizada de esta clase de imágenes de menores (sin que se distribuyan) implica que el fotógrafo es autor del delito que examinamos y el menor fotografiado la víctima del delito. El delito se consuma con la mera toma de la fotografía del menor y de sus partes íntimas. Esta toma fotográfica o captación de su imagen implica, a nuestro modo de ver, una producción de las mismas*"[11].

Las conductas típicas mencionadas hacen referencia a cualquier representación de un menor de 18 años de edad dedicado a actividades sexuales explícitas o a toda representación de sus partes genitales con fines predominantemente sexuales. Dos notas para destacar: una, por "partes genitales" se entiende los órganos sexuales externos; y, dos, la exigencia de la finalidad sexual excluye otras significaciones de esa representación, quedando las valoraciones artísticas al margen de un eventual juicio estético[12].

Con una pena menor que la prevista para el tipo penal básico se castiga, en el segundo párrafo, a quien tuviere en su poder representaciones de las descriptas antes[13].

Internet. La Cámara, que interpreta el art. 128 CP anterior a la reforma de la ley 26.388, afirma que "*si bien se ha comprobado fehacientemente que E.M., ha remitido dos fotografías con imágenes de menores (...), ello no alcanza, a criterio del tribunal, para afirmar la tipicidad de la conducta del nombrado. El texto del delito previsto y reprimido por el párrafo segundo del artículo 128 del Cód. Penal, claramente hace referencia -como acción típica- a la distribución del material pornográfico. Es decir, no pune el simple y único envío a una persona determinada. Así pues, es claro que el accionar de M. -envío en forma privada y a una única persona de las fotografías- no es delito, pues no constituye la realización del verbo típico*".

10. ABOSO (2020) apdo. 10.

11. PALAZZI (2016) p. 31.

12. ABOSO (2020) apdo. 8. Además, la representación alude a cualquier imagen, fotografía, dibujo o vídeo que cumpla con los requisitos señalados en el tipo penal, no siendo necesario que sea una imagen entera.

13. DUPUY (2018) p. 92. Dice: "*En poco tiempo, la figura del vendedor de pornografía infantil fue sustituida por la de consumidores que se asocian sin ánimo de lucro, bajando, subiendo y facilitando cantidad de archivos de contenido pornográfico infantil rápidamente y ayudados por las técnicas avanzadas de la tecnología -red peer to peer*". Y agrega: "*Hoy la situación es incontrolable y es fundamental abordar la problemática desde la prevención, correcta legislación y sin dejar de observar el tratamiento en otros países, pues una de las características fundamentales de los delitos que se llevan a cabo en entornos digitales es la transnacionalidad*".

Es decir, se castiga la simple tenencia dolosa de pornografía de menores de 18 años. Esta constituye la principal modificación introducida en 2018, pues la simple tenencia de tal material sin la finalidad distributiva o comercial configuraba un hecho atípico con la anterior redacción del tipo penal[14].

El tercer párrafo castiga al que tuviere en su poder las representaciones a las que hace alusión el primer párrafo, con fines inequívocos de distribución o comercialización. Resolver cuándo hay finalidad inequívoca de distribución o comercialización puede no ser sencillo, y más allá de que las circunstancias del caso serán las que definirán la presencia o no de este singular propósito, en el mundo digital es fácil poseer un archivo y realizar copias en forma instantánea. Por ende, la finalidad de distribuirlas no surgirá de la cantidad de imágenes secuestradas, sino de otros elementos y circunstancias que estarán presentes en el caso concreto. El legislador penal indica, además, que esta finalidad debe ser "inequívoca", por lo que solo el contexto del caso permitirá al juzgador concluir si se está o no en presencia de dicho propósito[15].

El cuarto párrafo del artículo 128 dice: "*Será reprimido con prisión de un mes a tres años el que facilitare el acceso a espectáculos pornográficos o suministrare material pornográfico a menores de catorce años*". Aquí, la conducta disvaliosa que describe la norma consiste en facilitar el acceso a espectáculos pornográficos o suministrar material de esa índole a menores de 14 años. El concepto "material" es más abarcativo que el de "imágenes", pues comprende no solo las imágenes, sino también las esculturas, películas, objetos de variada índole, descartándose cualquier material de carácter científico o auténticas obras de arte[16].

La ley 27.436 introduce el último párrafo en el artículo 128 por medio del cual se incrementa la escala penal cuando el sujeto pasivo del delito fuera menor de 13 años. Este incremento penológico resulta razonable, pues el menor de 13 de años se encuentra en una situación de extrema vulnerabilidad. Este agravamiento de pena, asimismo, se corresponde con la edad prevista en otros delitos contra la integridad sexual en los que la intangibilidad sexual de los menores de 13 años se presume *iure et de iure*, pues carecen de suficiente capacidad para comprender la dimensión de actividades con connotación sexual[17].

14. Consúltese, ampliamente, RIQUERT (2018a).

15. PALAZZI (2016) p. 37.

16. ABOSO (2020) apdo. 6: "*En el caso de las obras de arte, habrá de analizarse en cada caso si las imágenes de menores de edad guardan relación inequívoca con lo pornográfico o, por el contrario, si tal representación puede ser relacionada con ciertas formas de expresión artística que incluya a menores de edad, lo mismo ocurre muchas veces con algunas imágenes fotográficas de menores de edad (por lo general orillando los diecisiete años) asumiendo conductas eróticas o sexuales, en especial, durante el período estival. Primeramente, la doctrina había distinguido la pornografía y el arte por separado, pero en los últimos tiempos se ha admitido que la pornografía también puede ser arte*".

17. Tipos penales contemplados en los arts. 119 (abuso sexual), 125 y 128 a 130 (corrupción de menores), del Código penal argentino.

2. Ciberacoso sexual de menores (art. 131 CP)

La ley 26.904, sancionada el 13 de noviembre 2013, incorpora en el artículo 131 el delito conocido como *grooming*[18], que prevé lo siguiente: "*Será penado con prisión de seis (6) meses a cuatro (4) años el que, por medio de comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos, contactare a una persona menor de edad, con el propósito de cometer cualquier delito contra la integridad sexual de la misma*"[19].

La acción típica consiste en tomar contacto con una persona menor de edad por cualquier tecnología de transmisión de datos, con el propósito de entablar con el o la menor de edad, un acercamiento para cometer un delito contra su integridad sexual. Es requisito indispensable que el contacto haya sido realizado por medios de telecomunicación, es decir que se haya dado en un entorno virtual. Si se diera en el mundo real, en todo caso, estaríamos ante una tentativa o un acto preparatorio impune[20].

El tipo penal omite distinguir, en el caso del sujeto activo, entre mayores y menores, es decir que, con la vigente redacción, agente puede serlo tanto un mayor como un menor de edad[21]. Sujeto pasivo será, exclusiva y solamente, una persona menor de edad.

Ahora bien, es posible sostener que estamos frente al castigo penal de un acto preparatorio, por lo que el estudio de la tipicidad de la conducta se debe completar con la intención de cometer un delito contra la integridad sexual del sujeto pasivo, es decir, debe verificarse la existencia de un determinado propósito en la ejecución del comportamiento típico[22]. Lo anterior, claro está, con la consabida dificultad probatoria que implica su equivocidad y el peligro que representa la extensión del universo punitivo[23].

---

18. Cuando hablamos de *grooming* hacemos referencia a "t*odas las prácticas desplegadas en línea por ciertos adultos, pederastas y pedófilos, conocidos en la red como 'groomer', para ganarse la confianza de un menor fingiendo empatía, cariño, etc. normalmente bajo una falsa identidad de otro menor, con la finalidad de satisfacer sus apetencias sexuales*". Véase VANINETTI (2013) p. 1.

19. Ampliamente, al respecto, RIQUERT (2014).

20. GRISETTI (2016) p. 1.

21. Esto no se corresponde con lo que se entiende por *grooming*, pues éste presupone que quien contacta al menor es un mayor de edad. Al respecto, véase, GRENNI y FERNÁNDEZ RÍOS (2018) p. 110.

22. En este sentido, alguna doctrina ha sostenido que la voluntad del legislador con este precepto fue adelantar la barrera de tutela con la incriminación de conductas que se caracterizan como actos preparatorios de delitos sexuales contemplados en código de fondo argentino. Al respecto, véase BUOMPADRE (2014).

23. RIQUERT (dir.) (2018b) p. 858.

Este tipo penal admite únicamente la modalidad dolosa de comisión y, además, contiene un especial elemento subjetivo distinto del dolo que consiste -como se dejó dicho con la reproducción del texto legal- en contactar a un menor de edad con el fin de cometer cualquier delito contra su integridad sexual[24].

El delito se consuma cuando se establece efectivamente contacto con el menor de forma tal que sea advertible o manifiesto el propósito ilícito de la comunicación, pues no se trata del reproche penal de cualquier contacto, sino únicamente de uno que persiga el propósito indicado[25].

3. Violación de correspondencia digital (art. 153 CP)

El artículo 153 del Código penal argentino, conforme a la redacción dada por la ley 26.388, en su primer párrafo, dispone: "*Será reprimido con prisión de quince días a seis meses el que abriere o accediere indebidamente a una comunicación electrónica, una carta, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, que no le esté dirigido; o se apoderare indebidamente de una comunicación electrónica, una carta, un pliego, un despacho u otro papel privado, aunque no esté cerrado; o indebidamente suprimiere o desviare de su destino una correspondencia o una comunicación electrónica que no le esté dirigida*".

Por un lado, la acción de acceso o apertura configura el acto típico mediante el cual se viola el secreto de la correspondencia, abriendo o accediendo "*indebidamente a una comunicación electrónica, una carta, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, que no le esté dirigido*". La acción de abrir se materializa con la remoción de obstáculos que impiden la lectura de su contenido. Aplicado a la comunicación electrónica, este acceso o apertura indebida puede tener lugar en diversos puntos de una red y de ello dependerá, entonces, cómo se materializa. Por ejemplo, ingresar a la cuenta de correo electrónico de una persona y revisar en su carpeta de mensajes enviados un correo que no le estaba dirigido, o en la carpeta de mensajes recibidos y acceder a dicho contenido. La apertura o acceso, como indica el legislador, debe ser realizada "indebidamente" –término que a primera vista parece ser un tanto sobreabundante en la redacción del delito–, es decir, sin derecho.

Por otro lado, el tipo penal prevé la acción típica de apoderarse indebidamente de una comunicación electrónica, una carta, un pliego, un despacho u otro papel privado, aunque no se encuentre cerrado. La doctrina ha dicho –postura que se comparte– que "(p)*ese a las clásicas opiniones doctrinarias, entendemos que el término 'apoderarse' no debería seguir requiriendo los elementos propios del hurto cuando es aplicado a ambientes digitales. Ello así pues si el legislador incluyó un objeto (el correo*

24. GRISETTI (2016) p. 1.

25. RIQUERT (dir.) (2018b) p. 858.

electrónico o, en forma más general, la comunicación electrónica) del cual el sujeto activo puede apoderarse (copiar) sin desapoderar. Entendemos que la interpretación debe acompañar la intención de sancionar la conducta descripta"[26].

La figura penal comentada, además, castiga a quien "*indebidamente suprimiere o desviare de su destino una correspondencia o una comunicación electrónica que no le esté dirigida*". Por ello, el delito consiste en impedir que la correspondencia en curso y no dirigida al agente llegue a su destinatario, sea sacándola (supresión) o cambiándola (desvío) de curso[27].

El artículo 153 en su segundo párrafo castiga a quien "*indebidamente interceptare o captare comunicaciones electrónicas o telecomunicaciones provenientes de cualquier sistema de carácter privado o de acceso restringido*"[28]. La acción típica consiste en interceptar o captar comunicaciones electrónicas o telecomunicaciones provenientes de cualquier sistema de carácter privado o de acceso restringido, y objeto del delito son las "*comunicaciones electrónicas o telecomunicaciones provenientes de cualquier sistema de carácter privado o de acceso restringido*".

Asimismo, el artículo, en su párrafo tercero, dice que "(l)*a pena será de prisión de un mes a un año, si el autor además comunicare a otro o publicare el contenido de la carta, escrito, despacho o comunicación electrónica*". La reforma que modificó este precepto sustituyó el término "culpable" por "autor", siendo ello lógico, pues muy distinto es ser autor de un hecho que culpable del mismo[29] y, además, incorporó la "comunicación electrónica"[30].

Finalmente, la disposición regula una circunstancia que agrava el castigo penal cuando establece que "(s)*i el hecho lo cometiere un funcionario público que abusare de sus funciones, sufrirá además, inhabilitación especial por el doble del tiempo de la*

26. PALAZZI (2016) p. 52.

27. PALAZZI (2016) p. 53. Dice: "*Entendemos que ella está en curso mientras el destinatario final no la haya 'bajado' del servidor y no la haya abierto, es decir, no ha tomado conocimiento de ella. Incluso la comunicación puede haber llegado efectivamente a su casilla, pero podrá suceder que aquél no haya revisado aún su casilla de correo electrónico o su voice mail. El autor del hecho (alguien con acceso, como el administrador de la red) puede suprimir dolosamente el correo electrónico efectivamente recibido, pero no abierto. Todo ello será cuestión de prueba y dependerá, en gran medida, de la configuración de la red y del sistema de correo*".

28. Con este nuevo párrafo se pretende castigar las escuchas telefónicas ilegales, que hasta la sanción de la reforma no configuraban delito en la Argentina, salvo por el caso de una norma especial en la ley 25.520 de Inteligencia Nacional, que resultaba aplicable únicamente a los agentes de inteligencia (arts. 42 y 43).

29. POLAINO NAVARRETE (2016) pp. 179- 236 y ss.

30. La diferencia con el art. 155 CP, que analizaremos luego, es que aquí el autor de la publicación es al mismo tiempo el de la apertura o apoderamiento de la comunicación electrónica. Si el que publica es un tercero, resultará aplicable el art. 155 CP, y si la publicación fue hecha con el propósito de defender un interés público, encontrará tutela en el segundo párrafo de dicha disposición.

condena". El agravamiento de pena tiene sentido, ya que la realización del tipo penal por funcionarios públicos afecta la mayor responsabilidad y culpabilidad de estos sujetos que abusan de la facilidad que le brinda su propio rol funcional[31].

4. Acceso ilegítimo a datos o a sistema informático (art. 153 bis CP)

La ley 26.388 incorporó el artículo 153 bis al Código penal que en su primer párrafo dispone: "*Será reprimido con prisión de quince días a seis meses, si no resultare un delito más severamente penado, el que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido*".

Antes de comentar algunos extremos de configuración de este delito, recordemos que por "dato informático" se entiende a la unidad mínima de información sometida a tratamiento informático o automatizado. Y, por "sistema informático", al dispositivo aislado o conjunto de dispositivos interconectados que aseguran, mediante la ejecución de un programa o software, el tratamiento automatizado de datos[32].

La aplicación de este tipo penal es subsidiaria. La acción típica, que consiste en acceder por cualquier medio a un sistema o dato informático de ingreso restringido, puede significar el comienzo material de otro proceso criminal (como estafa, daño o sustracción de datos personales), razón por la cual el legislador dispuso que solo resultará de aplicación esta figura si no resultare un delito más severamente penado.

Resulta lógico, por otro lado, que el texto legal se refiera a los sistemas o datos informáticos de acceso restringido, pues el acceso a sistemas o redes abiertas, o al contenido publicado en un sitio de Internet de acceso público, no configura un comportamiento prohibido por la ley. Será de acceso restringido un sistema o dato informático por contar con alguna medida de seguridad que impida el libre ingreso y que tendrá que sortearse para ingresar. Cualquier otra interpretación conduciría al absurdo de sancionar a quienes navegan por Internet entrando a sitios públicos[33].

Y, algo más sobre lo último. El vocablo "restringido" se opone a libre acceso, y no debe entenderse como un elemento fáctico, sino como un elemento normativo del tipo penal: cualquier persona con conocimientos avanzados de informática puede acceder a un ordenador ajeno conectado a Internet, lo que sucede con habitualidad, es una posibilidad, pero no debe hacerlo, porque es propiedad ajena. El vocablo "restringido" se refiere a la obligación de no ingresar en un ordenador ajeno[34].

31. SUERIO (2015) p. 105.

32. Definiciones recogidas en el art. 1 (a y b) del Convenio sobre la Ciberdelincuencia (Budapest, 23 de noviembre de 2001). La República Argentina adhirió al Convenio por medio de la Ley 27.411 de 22 de noviembre de 2017.

33. PALAZZI (2016) p. 65.

34. LUCERO y KOHEN (2015) p. 85.

El tipo penal bajo análisis castiga la entrada por cualquier medio, por lo que el acceso no necesariamente debe ser remoto. No requiere ninguna acción adicional, como copiar o suprimir o reenviar datos, es decir, se consuma por el mero acto de acceder a un sistema o dato informático de ingreso restringido, con independencia de que luego se cometan otros delitos[35].

Asimismo, el artículo 153 *bis* dispone en su segundo párrafo que "(l)*a pena será de un mes a un año de prisión cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros*". Con este último párrafo, el legislador incrementa la escala penal de la figura legal básica por considerar que el acceso en perjuicio de un sistema o dato informático de un organismo público estatal, o de un proveedor de servicios públicos o financieros, configura un supuesto que merece una protección penal especial[36].

5. Publicación ilegal o abusiva de comunicación electrónica (art. 155 CP)

La redacción dada por ley 26.388 al artículo 155 reprime con multa al "*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*".

La otrora disposición castigaba la publicación indebida de correspondencia, la revelación del secreto profesional y la de hechos, actuaciones o documentos que por la ley deban quedar secretos. Hoy, tras la reforma de 2008, se castiga también a quien publica una comunicación electrónica[37].

El sujeto activo del delito es el que la da a conocer encontrándose en posesión de la comunicación electrónica. El ofendido por este delito, por otro lado, es el remitente, porque es él quien tiene derecho de disponer de lo que comunica, pero también se ha dicho que el destinatario puede ser ofendido cuando un tercero hace la publicación, e incluso se le atribuye esa calidad al tercero perjudicado por la publicación[38].

El objeto del delito es la correspondencia, es decir, toda comunicación electrónica, pliego cerrado, despacho telegráfico, telefónico o de otra naturaleza, no destinados a la publicidad dirigido por una persona a otra u otras, que exprese pensamientos e ideas por ese medio[39].

35. RIQUERT (dir.) (2018b) p. 1163.
36. LUCERO y KOHEN (2015) p. 90.
37. RIQUERT (dir.) (2018b) p. 1172.
38. LUCERO y KOHEN (2015) p. 92.
39. RIQUERT (dir.) (2018b) p. 1175.

Por otro lado, la ilegitimidad del hecho resulta del juego de las expresiones "indebidamente" y "no destinada a la publicidad". Por ello, deja de ser indebida la publicidad cuando median causas de justificación o el consentimiento del remitente que, en este caso, es el interesado. La publicación de la correspondencia con consentimiento de la víctima implica que quien la difunde actúa debidamente y por eso no comete el delito que venimos estudiando[40].

Se agrega un segundo párrafo al artículo 155, que regula un supuesto de exención de responsabilidad penal: "*Está exento de responsabilidad penal el que hubiere obrado con el propósito inequívoco de proteger un interés público*". En verdad, este supuesto permite al agente demostrar el interés público de lo que ha publicado y, en tal caso, verse exento de responsabilidad penal[41].

6. Revelación de secretos oficiales (art. 157 CP)

En consonancia con las reformas introducidas en los artículos 153 y 155 arriba analizados, se sustituye el artículo 157 del Código penal por el siguiente texto: "*Será reprimido con prisión de un mes a dos años e inhabilitación especial de uno a cuatro años, el funcionario público que revelare hechos, actuaciones, documentos o datos, que por ley deben ser secretos*".

El tipo penal bajo análisis, cuya acción típica consiste en revelar hechos, actuaciones, documentos o datos que por ley deben ser secretos, se configura como un delito especial, restringiéndose en consecuencia el círculo de sujetos activos al funcionario público que se encuentre en la obligación de guardar un secreto.

El legislador ha incorporado a los "datos" con el fin de proteger información almacenada en un sistema digital, requiriendo que esos datos tengan el carácter de secretos. Denominamos datos a "*cualquier medio de información ya sea electrónico, en soporte papel y/o cualquier otro soporte idóneo. El llamado dato electrónico abarca a bases, archivos, documentos de texto, imágenes, voz y video codificados en forma digital*"[42].

Con acierto se ha dicho que "*el tipo penal requiere una norma expresa que diga que esos datos son secretos. Es que el principio general en la Administración pública es la transparencia y publicidad de actos y documentos de gobierno (lo que incluye datos), por lo que una pauta adecuada para determinar qué es secreto y qué no lo es deberá recaer necesariamente en exigir una ley que así lo disponga. Solo de esta manera se salva el principio de taxatividad penal*"[43].

40. PALAZZI (2016) p. 75.

41. Al respecto, solo un breve comentario: estar exento de responsabilidad penal no significa que no haya delito. Véase, sobre supuestos de exención de responsabilidad penal, POLAINO NAVARRETE (2016) pp. 22 y 168 y s.

42. Ampliamente, SORBO (2013).

43. PALAZZI (2016) p. 31.

Nos encontramos frente a un tipo penal que se configura con el conocimiento por parte del agente de que el dato es secreto y que su divulgación se encuentra prohibida, por lo cual únicamente resulta típica la modalidad dolosa de este delito[44].

Se admite la tentativa en este delito, pero cierto es que su prueba es sumamente compleja, pues aquélla se produce cuando el tercero toma conocimiento del secreto sin que se produzca el daño. Si se produce tal daño, salimos de la figura de la tentativa. Dicho lo anterior de otro modo, si el secreto se mantiene "guardado" en el tercero que no debe conocerlo y no se puede probar que ese secreto fue suministrado por el funcionario público, estamos frente a una prueba imposible[45].

7. Acceso ilegítimo, difusión o alteración de datos personales (art. 157 bis)

La ley 26.388 modifica el artículo 157 *bis*, que queda redactado de la siguiente manera: "*Será reprimido con la pena de prisión de un mes a dos años el que: 1) a sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales; 2) ilegítimamente proporcionare o revelare a otro información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley; 3) ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales. Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de uno a cuatro años*".

El tipo penal reprime a quien ingrese a un banco de datos personales sin autorización ni permiso alguno, a quien revelare secretos o archivos obrantes en ese banco de datos y a quien los modifique por cualquier medio. Se agrava la pena si el sujeto activo es un funcionario público[46].

La figura del inciso primero consiste en acceder ilegítimamente y a sabiendas, de cualquier forma, a un banco de datos personales[47], siendo claro que solo se admite la modalidad dolosa de este tipo penal. Además, de acuerdo con la redacción del tipo penal, se puede cometer "o violando sistemas de confidencialidad y seguridad de datos". Sostenemos que esta conjunción alternativa ("o") carece de sentido, pues la expresión en la figura "a sabiendas e ilegítimamente" no puede operar como una

44. RIQUERT (dir.) (2018b) p. 1208.

45. LUCERO y KOHEN (2015) p. 99.

46. Esta figura se encuentra estrechamente relacionada con la protección de datos personales establecidos en la Ley 25.326, de 2000, que incorporó las figuras del acceso ilegítimo a un banco de datos y revelación ilegítima de información.

47. La Ley 25.326, de 2000 (Protección de Datos Personales), en su art. 2 define el archivos, registro, base o banco de datos de la siguiente forma: "*Indistintamente, designan al conjunto organizado de datos personales que sean objeto de tratamiento o procesamiento, electrónico o no, cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso*".

alternativa a la modalidad comisiva "violando sistemas de confidencialidad y seguridad de datos". No solo eso, sino que tal violación implica un "a sabiendas¨, como dice la figura, lo que igualmente ya estaba implícito. Entonces, el "o" puede interpretarse únicamente como una opción y no como alternativa a cuando no se actúe a sabiendas e ilegítimamente, elementos que, para que se configure este tipo penal, deben estar presentes[48].

El segundo inciso de la disposición castiga al que ilegítimamente proporcione o revele 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. En la modificación del inciso se incorporó el vocablo "archivo" y la expresión "ilegítimamente proporcionare", términos que no estaban previstos en la otrora disposición.

Con el primer añadido, la información registrada, además de poder encontrarse en un banco de datos personales, puede hallarse en un simple "archivo", lo que permite alcanzar a un universo mayor de conductas. El verbo "proporcionar" consiste en hacer lo necesario para que una persona tenga algo que necesita, facilitándoselo o dándoselo, y el tipo penal exige que el agente se encuentre obligado a preservar la información[49].

Por otro lado, el término "ilegítimamente" reclama estudiar si la revelación de los datos es o no legítima de acuerdo al sistema normativo vigente. Ello alude al cumplimiento de la ley 25.326 y sus reglamentaciones, que es el cuerpo normativo que regula el uso de datos personales en el ordenamiento jurídico argentino[50].

El último inciso sanciona al que "*ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales*". Este comportamiento se encontraba castigado con algunas diferencias en el artículo 117 *bis* del Código penal, siendo la nueva ubicación en el articulado una decisión motivada en identificar la modalidad delictiva estudiada con la tutela del honor en el caso de afectación de datos falsos[51].

La novedad que trae consigo la ley 26.388 con este tercer y último inciso radica en la eliminación del término "falsos", decisión legislativa que ha sido explicada del siguiente modo: "*Pareciera que la conducta reprochada podría encontrarse alcanzada por las previsiones legales del artículo 117 bis. Sin embargo, si bien este artículo en su inciso 1° reprime con pena de prisión de un mes a dos años al que "insertara o hiciera insertar a sabiendas datos falsos en un archivo de datos personales", no puede soslayarse su ubicación sistemática dentro del Código Penal, por lo que si tene-*

48. PALAZZI (2016) p. 88.

49. CHERÑAVSKY *et al.* (2018) p. 145.

50. Ello importa tener muy en claro que la ley 25.326 está compuesta por una serie de principios generales como el consentimiento, la cesión de datos y, también, por regímenes especiales (arts. 25, 26 y 27).

51. LUCERO y KOHEN (2015) p. 164 y s.; PALAZZI (2016) p. 91.

mos en cuenta el bien jurídico protegido por el título la nueva figura parece limitarse sólo a la inserción de datos falsos que disminuyan el honor. Por tal motivo, la única interpretación adecuada del citado artículo, es la de considerar que contempla las acciones que desacreditan o deshonran, pese a que ello no surge del texto de la ley"[52].

8. Estafa o fraude informático (art. 173, inc. 16 CP)

La ley 26.388 incluyó en el artículo 173 del Código penal, como nuevo inciso 16, el siguiente texto: "*El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos*".

Con esta nueva modalidad de defraudación se pretende dar respuesta a algunas situaciones patrimoniales abusivas relacionadas con la informática, y superar el problema vinculado a la imposibilidad de estafar a una máquina u ordenador[53]. Así, justamente, "*desaparecen las hipótesis de atipicidad que se daban por no concurrir en el caso concreto la secuencia tradicional de la estafa (ardid o engaño, error, disposición patrimonial perjudicial), en especial el engaño a otro a que hace referencia el art. 172 del Cód., que requiere para su determinación el engaño a otra persona física*"[54].

El inciso 16 del artículo 173 recepta una nueva modalidad de estafa informática que tiene lugar "*mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos*". Con esa expresión, el legislador parece abarcar un amplio abanico de posibilidades, restringiendo sí la técnica: debe ser una "*que altere el normal funcionamiento de un sistema informático o la transmisión de datos*".

La acción genérica de alterar el normal funcionamiento puede recaer sobre un sistema informático o sobre la transmisión de datos, entendiéndose por este último supuesto el caso en que, sin alterar el sistema informático, se lo engaña en la recepción de información, por ejemplo, impidiendo el funcionamiento validación de datos[55].

52. En estos términos lo fundamentó la Cámara de Diputados de la Nación Argentina, en la 13° Reunión, continuación de la 5° Sesión ordinaria, de 4 de junio de 2008, en el marco del debate parlamentario de la Ley 26.388.

53. En estos términos lo fundamentó la Cámara de Diputados de la Nación Argentina, en la 13° Reunión, continuación de la 5° Sesión ordinaria, de 4 de junio de 2008: "*Con relación al 'fraude informático' existió coincidencia en cuanto a la conveniencia de incorporarlo dentro del capítulo sobre las defraudaciones, y despejar definitivamente las dudas suscitadas en los tribunales sobre en qué tipos de delitos contra la propiedad debe subsumirse la conducta*".

54. BUOMPADRE (2017) p. 476.

55. PALAZZI (2016) p. 181.

Además, para que se configure el tipo penal que venimos describiendo deben darse los elementos de la estafa: una disposición patrimonial por parte de la máquina o de un tercero que entrega un bien o el acceso a un servicio o información a la que no tenía derecho sin pagarlo según los términos del servicio. Y, como todo delito contra el patrimonio, requiere que exista perjuicio patrimonial y ello se debe producir mediante dicha disposición patrimonial.

Podríamos mencionar varias y diversas modalidades de estafa informática cuyo análisis excede lógicamente el objeto de este estudio, pero sí haremos una brevísima referencia al *phishing*, que es una modalidad que consiste en remitir un correo electrónico engañoso a un cliente para que revele información personal, como número de tarjeta de crédito o débito o clave de cuenta bancaria, a través de sitios *web* simulados o en una respuesta de correo electrónico[56]. Este delito, que se configura con el robo o sustracción de la identidad del sujeto pasivo, no parece ser el típico delito informático, siendo por ello un tema para un particular análisis, que como se dijo rebasa el contenido del presente.

9. Daño en datos y sistemas informáticos (art. 183 y 184 CP)

El artículo 10 de la ley 26.388 incorpora como segundo párrafo del artículo 183, el siguiente texto: "*En la misma pena incurrirá el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños*".

La reforma en cuestión buscó dar respuesta a una de las más sentidas discusiones, vinculadas al alcance de los tipos penales tradicionales de daño, particularmente en aquellos supuestos de modalidades de daño cometido mediante TIC. En el marco de esas discusiones, algunos autores sostuvieron que la tipificación del daño a una cosa mueble podría comprender alguna de las nuevas realidades, pero naturales fueron las objeciones de analogía, por lo que de *lege ferenda* se formularon otras propuestas: o el agregado en el tipo penal existente del término "intangible" a la lista de elementos pasibles de daño, o el dictado de una nueva ley especial[57].

El legislador penal de 2008 parece haber escuchado las voces que reclamaban una modificación en el sentido antes expuesto, adaptando la legislación penal a este fenómeno delictivo con la incorporación pertinente[58].

56. CHERÑAVSKY (2019); GRIS MUNIAGURRIA *et al*. (2018).

57. RIQUERT (dir.) (2018b) pp. 1592 y s.

58. Al respecto, consúltese sentencia dictada por la Cámara Nacional Criminal y Correccional de la Capital Federal, Sala VI, en el marco del caso *Pinamonti, Orlando M*. (1993). El resolutorio sostuvo que, si bien el *software* es una obra intelectual protegida por la ley Nº 11.723, de la propiedad intelectual, su desaparición o destrucción no estaba contemplada entre las conductas que esta ley

Cabe destacar que, en el contexto en el cual se ejecuta el delito (informático) se entiende por "destruir" o "inutilizar" la acción de eliminar definitivamente, es decir, sin posibilidad de recuperación. Que exista un sistema de *back-up* no modifica el delito de daño, pues la restauración requiere un esfuerzo que trae consigo la reparación del daño causado.

Y, en lo que su parte final se refiere, el tipo penal consagra un delito de peligro[59] pues dispone que quien vende, distribuye, hace circular o introduce en un sistema informático un "virus", aun cuando no se utilice, será sancionado penalmente. Es que salvo aislados casos en que hay un interés académico, esta clase de programa está indiscutiblemente destinado a dañar[60].

Analicemos, además, el artículo 184, que también experimentó un cambio con la ley 26.388, cuyos incisos 5 y 6 quedan redactados del siguiente modo: "*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".

El quinto párrafo regula un agravamiento de la sanción penal en virtud del objeto, cuyo alcance amplió la ley 26.388 con la inclusión de los "datos, documentos, programas o sistemas informáticos públicos". Se trata de un incremento de pena que responde al interés general en tono a la conservación de los objetos que menciona el precepto[61].

Con relación al inciso sexto, la doctrina ha señalado: "*He manifestado anteriormente que coincido en el agravamiento de la pena si los daños son sobre sistemas de servicios públicos que afectarán a la sociedad en su conjunto. Ahora bien, supongamos un ataque a los sistemas informáticos de energía (Edenor, Edesur), lo cual ocasiona que toda la Ciudad se vea gravemente afectada por un período de tiempo prolongado lo cual sin duda alguna podrá acarrear un sin número de problemas tanto a la población como quizá al propio sistema de seguridad nacional*"[62]. Por ello, la perfección

penaliza, por lo que tal comportamiento resulta atípico. Textualmente: "*Ello es así porque al no revestir la calidad de cosa -cosa es solo soporte- tampoco es aprehendida por la figura descripta en el art. 183 del Código Penal*".

59. POLAINO NAVARRETE (2016) p. 115.

60. PALAZZI (2016) p. 112.

61. HUÑIS (2007) p. 865.

62. LUCERO y KOHEN (2015) p. 145.

de un delito de daño informático agravado podría dar lugar también a la figura de estrago doloso, siendo por esto válida la postura que sostiene que debería haberse incorporado al artículo 186 del Código penal esta nueva figura[63].

Por lo demás, se ha dejado dicho que "*correspondería que una futura reforma prevea mayores penalidades tanto para los autores que atentan contra la integridad de dichos sitios como para los funcionarios encargados de su mantenimiento y actualización. En este sentido, resulta fundamental prever también una sanción penal para el incumplimiento a dichos deberes de mantenimiento y actualización los que deberán ser taxativamente enumerados*"[64].

10. Interrupción o entorpecimiento de comunicaciones electrónicas (art. 197 CP)

El artículo 197 del Código penal, modificado por la ley 26.388, dispone que: "*Será reprimido con prisión de seis (6) meses a dos (2) años, el que interrumpiere o entorpeciere la comunicación telegráfica, telefónica o de otra naturaleza o resistiere violentamente el restablecimiento de la comunicación interrumpida*".

El tipo legal castiga penalmente acciones que pueden configurar dos figuras autónomas entre sí: la primera, interrumpir o entorpecer la comunicación; y, la segunda, resistir violentamente su restablecimiento.

Por la primera figura señalada -interrumpir o entorpecer la comunicación-, entendemos el acto de estorbar, dificultar, retardar, obstaculizar, sin llegar a interrumpir el funcionamiento de los servicios de comunicación. La segunda figura, por su parte, que es resistir violentamente el restablecimiento del servicio de comunicación, tiene lugar a la postre de haber sido interrumpido dicho servicio e implica un despliegue de energía física contra la labor de las personas que buscan reconectar el sistema de telecomunicaciones dañado. Esta acción puede ser llevada a cabo por el mismo sujeto que interrumpió el servicio o por un tercero ajeno a tal conducta[65].

La ley 26.388 ha modificado el tipo penal con el agregado de la expresión "o de otra naturaleza", ampliando de este modo la configuración del delito. Tras la reforma de 2008, la figura ampara cualquier clase de comunicación, incluyendo las privadas, como el correo electrónico, la voz por medio de IP o los mensajes de chat o de texto a través de celulares (SMS)[66].

63. Art. 186 CP, que castiga a quien causare incendio, explosión o inundación. Véase LUCERO y KOHEN (2015) p. 145.

64. CHERÑAVSKY *et al.* (2018) p. 149.

65. RIQUERT (dir.) (2018c) pp. 1722 y s.

66. Tal incorporación se encuentra justificada, pues las comunicaciones resultan elementos indispensables en nuestra realidad: vivimos en la denominada "Sociedad de la Información", basada precisamente en las comunicaciones. En este sentido: SUERIO (2014) p. 10.

El delito se consuma con la verificación de la creación de un riesgo para la "seguridad común". Antes de ello, solo podemos considerar el castigo de la conducta en grado de tentativa[67].

11. Alteración de medios probatorios (art. 255 CP)

El artículo 255 del Código penal, tras la reforma de 2008, quedó redactado del siguiente modo: "*Será reprimido con prisión de un (1) mes a cuatro (4) años, el que sustrajere, alterare, ocultare, destruyere o inutilizare en todo o en parte objetos destinados a servir de prueba ante la autoridad competente, registros o documentos confiados a la custodia de un funcionario público o de otra persona en el interés del servicio público. Si el autor fuere el mismo depositario, sufrirá además inhabilitación especial por doble tiempo. Si el hecho se cometiere por imprudencia o negligencia del depositario, éste será reprimido con multa de pesos setecientos cincuenta ($ 750) a pesos doce mil quinientos ($ 12.500)*".

La redacción de la figura legal transcripta ha experimentado las siguientes modificaciones con la ley 26.388: *i*, se incorporó el verbo típico "alterar" con el fin de proteger los sistemas informáticos de cualquier tipo de modificación; *ii*, se incorporó, también, la expresión "en todo o en parte", resultando posible un menoscabo total o parcial, siempre definitivo, del objeto en cuestión; y, *iii*, el término "culpable" ha sido sustituido por "autor", siguiendo la técnica de reforma del artículo 153 antes comentado.

Los verbos típicos son sustraer, ocultar, destruir o inutilizar: "*sustrae quien saca la cosa de la esfera de custodia de la que se encuentra, aunque sea momentáneamente, sin que sea necesario exigir apoderamiento. Oculta quien la esconde. Y destruye quien la menoscaba materialmente. Inutilizar algo es tornarlo inidóneo para sus fines*"[68].

Por lo demás, este delito se configura como un delito común, por lo que cualquiera puede ser sujeto activo. Sujeto pasivo del delito es aquel que tiene la custodia de los elementos de prueba. Admite únicamente la modalidad dolosa, pues quien incurre en el comportamiento típico lo hace a sabiendas del carácter de medios probatorios de los elementos en custodia.

El delito se consuma cuando, mediante la comisión de alguna de las conductas típicas, se quebranta la custodia de los objetos a cargo del agente. Y este tipo penal admite tentativa, pues si la alteración permite su recuperación, la prueba seguiría intacta[69].

67. RIQUERT (dir.) (2018c) p. 1724.

68. RIQUERT (dir.) (2018c) p. 1987.

69. LUCERO y KOHEN (2015) p. 158.

12. Otros tipos penales facilitados por TIC

Dispersos en el articulado del Código penal y sin una ordenación sistemática común y homogénea, encontramos otros tipos penales que utilizan TIC para la comisión[70]. En este sentido, "(n)*o hay que perder de vista que como correlato del avance de Internet en gran parte en nuestras interacciones sociales, los delitos tradicionales actualmente son reproducidos y cometidos a través de las tecnologías de la información y la comunicación (TICs), dado que el medio digital les ha permitido ampliar el espectro de destinatarios y por ende llegar a mayor número de víctimas en menor tiempo y sin necesidad de inmediación física, con el solo requisito de poseer un dispositivo conectado a la red*"[71].

Sin ánimo exhaustivo o de *numerus clausus*, podemos mencionar los siguientes delitos regulados en el Código penal argentino, sumergidos en ese universo de cibercriminalidad: calumnia o falsa imputación (artículo 109), injuria (artículo 110), publicaciones obscenas y corrupción de menores (artículos 125 a 128), trata de personas menores de edad (artículos 145 *bis* y 145 *ter*), amenazas (artículo 149 *bis*), divulgación de secretos (artículo 156), extorsión (artículo 168), chantaje o amenaza de imputaciones contra el honor o violación de secretos (artículo 169), defraudación haciendo suscribir con engaño algún documento (artículo 173, inciso 3), estafa procesal (artículo 173, inciso 8), comercialización y suministros de medicamentos sin autorización (artículo 209), intimidación pública (artículo 211 y 212) y apología del delito (artículo 213).

III. Reflexiones finales

1. Los delitos informáticos no responden más que a la adaptación del ordenamiento jurídico-penal a una nueva realidad construida por la cultura TIC, siendo por ello un fiel reflejo de la sociedad tecnológica imperante derivada de la simbiosis entre Derecho y nuevas tecnologías.
2. La sinergia Derecho y nuevas tecnologías plantea nuevos interrogantes y desafíos jurídico-penales que reclaman una reformulación de la configuración clásica que hasta ahora teníamos del Derecho penal. Aquella conjunción, supondrá el futuro de una nueva disciplina científica objeto de análisis para los juristas, y con ella, naturalmente, una nueva especie de delitos informáticos.
3. La criminalidad informática no es ignorada por el legislador penal argentino: su realidad y presencia son incuestionables, y los efectos ocasionados pueden resultar demoledores. En este contexto, el moderno Derecho penal ha de combatir estas nue-

70. SAÍN (2018) p. 46. Agrega el autor: "*Los delitos informáticos, en cambio, son todos aquellos hechos ilícitos que utilizan como medio y como fin algún dispositivo informático para su comisión*".
71. CHERÑAVSKY *et al.* (2018) p. 152.

vas prolíficas manifestaciones delictivas, especialmente por medio de eficaces medidas de prevención criminal, al servicio de las exigencias de la estabilidad y salvaguarda de los valores reconocidos en la sociedad actual.

Referencias bibliográficas

ABOSO, Gustavo (2020): "La nueva regulación del delito de distribución de pornografía infantil a la luz de la reforma de la ley 27.436 (Art. 128 del Código Penal argentino)". Disponible en: elDial.com - DC2A5C. [Fecha de consulta 27 de julio de 2020].

BUOMPADRE, Jorge (2017): *Manual de Derecho Penal. Parte especial*, 3° reimpresión, Editorial Astrea, Buenos Aires.

BUOMPADRE, Jorge (2014): "*Grooming*". Disponible en: http://www.pensamientopenal.com.ar/doctrina/40272-grooming. [Fecha de consulta: 23 de junio de 2020].

CHERÑAVSKY, Nora (2019): *"Falsos perfiles en internet y derecho penal"*. En *Temas de Derecho penal y procelas penal* (Buenos Aires, Editorial Erreius) pp. 227-239.

CHERÑAVSKY, Nora, GRIS MUNIAGURRIA, Pablo y MOREIRA, Diógenes (2018): *"A diez años de la ley de delitos informáticos. Balance y propuestas"*. En *Sistema penal e informática. Ciberdelitos. Evidencia digital. Tics* (Buenos Aires, Editorial Hammurabi, volumen 1), pp. 129-160.

DUPUY, Daniela (2018): *"La pornografía infantil y la tenencia recientemente legislada"*. En *Cibercrimen y delitos Informáticos: los nuevos tipos penales en la era de Internet*, Suplemento Especial (Buenos Aires, Editorial Erreius), pp. 91-100.

FIGARI, Rubén (2018): "Comentario al art. 128 del C.P. (Ley 27.436) sobre pornografía infantil". Disponible en: http://pensamientopenal.com.ar/doctrina/47068-comentario-al-articulo-128-del-codigo-penal-ley-27436-sobre-pornografia-infantil. [Fecha de consulta: 23 de junio de 2020].

GRENNI, Lucas y FERNÁNDEZ RÍOS, Rodrigo (2018): *"La previsión normativa del tipo penal de grooming en la Argentina"*. En *Cibercrimen y delitos Informáticos: los nuevos tipos penales en la era de Internet*, Suplemento Especial (Buenos Aires, Editorial Erreius), pp. 101-120.

GRISETTI, Ricardo (2016): *"El grooming. Una nueva modalidad delictual"*. En *Revista Jurídica Argentina La Ley*, La Ley, tomo 2016-D, Julio de 2016.

GRIS MUNIAGURRIA, Pablo, CHERÑAVSKY, Nora y MOREIRA, Diógenes (2018): *"'Phishing': abordaje del fenómeno desde la prevención y la investigación"*. En *Sistema penal e informática. Ciberdelitos. Evidencia digital. Tics* (Buenos Aires, Editorial Hammurabi, volumen 2), pp. 117-135.

HUÑIS, Ricardo (2007): "Comentario a los artículos 183/184". En *Código penal y normas complementarias. Análisis doctrinal y jurisprudencial* (Buenos Aires, Editorial Hammurabi, tomo VII), pp. 825-847.

LUCERO, Pablo y KOHEN, Alejandro (2015): *Delitos informáticos* (Buenos Aires, Editorial Albrematica).

PALAZZI, Pablo (2016): *Los Delitos Informáticos en el Código Penal. Análisis de la ley 26.388* (Buenos Aires, Editorial Abeledo Perrot, 3° edición actualizada y ampliada).

POLAINO NAVARRETE, Miguel (2016): *Lecciones de Derecho penal, Parte general* (Madrid, Editorial Tecnos, tomo II, 2a. edic. corregida y actualizada).

RIQUERT, Marcelo (2020): *"Difusión inconsentida de imágenes sexuales de tercero en tiempos de pandemia".* Disponible en: elDial.com - DC2B37. [Fecha de consulta: 28 de julio de 2020].

RIQUERT, Marcelo (2018a): *"Tenencia simple de pornografía infantil y figuras conexas"*. En *Cibercrimen y delitos Informáticos: los nuevos tipos penales en la era de Internet*, Suplemento Especial (Buenos Aires, Editorial Erreius), pp. 69-90.

RIQUERT, Marcelo (dir.) (2018b): *Código Penal de la Nación. Comentado y Anotado* (Buenos Aires, Editorial Erreius, Tomo II).

RIQUERT, Marcelo (dir.) (2018c): *Código Penal de la Nación. Comentado y Anotado* (Buenos Aires, Editorial Erreius, Tomo III).

RIQUERT, Marcelo (2014): *"El 'cibergrooming': nuevo art. 131 del CP y sus correcciones en el 'Anteproyecto' argentino de 2014".* En *Revista de Derecho Penal y Criminología*, La Ley, año IV, N° 1, febrero de 2014. Disponible en: http://www.pensamientopenal.com.ar/system/files/2017/04/doctrina45151.pdf. [Fecha de consulta: 26 de julio de 2020].

SAÍN, Gustavo (2018): *"La estrategia gubernamental frente al cibercrimen: la importancia de las políticas preventivas más allá de la solución penal"*. En *Cibercrimen y delitos Informáticos: los nuevos tipos penales en la era de Internet*, Suplemento Especial (Buenos Aires, Editorial Erreius), pp. 7-32.

SORBO, Hugo (2013): *"Delitos Informáticos. Aspectos a tener en cuenta de la Ley 26.388"*. Disponible en: http://server1.utsupra.com/doctrina1?ID=articulos_utsupra_02A00376672921. [Fecha de consulta: 13 de julio de 2020].

SUERIO, Christian (2018): *"Ciberataques y la propuesta del Anteproyecto de reforma integral al Código Penal de la Nación"*. Disponible en: elDial.com - DC263A. [Fecha de consulta: 20 de junio de 2020].

SUERIO, Christian (2015): *Criminalidad informática* (Buenos Aires, Editorial Ad-Hoc).

SUERIO, Christian (2014): *"La criminalidad informática en el proyecto de ley de reforma, actualización e integración al Código Penal de la Nación"*. En *Revista de Derecho Penal y Criminología*, La Ley, Nº 6, pp. 10-40.

VANINETTI, Hugo (2013): *"Inclusión del 'grooming' en el Código Penal"*. En *Revista Jurídica Argentina La Ley*, La Ley, tomo 2013-F-1200, diciembre de 2013.