Delitos informáticos en Argentina

Normativa actual y posibilidades de cambio según el proyecto de nuevo Código Penal

Daniel Schurjin Almenar [1]

SUMARIO: I.- Introducción II.- Legislación argentina vigente en materia de delitos informáticos y propuestas de actualización mediante el proyecto de nuevo Código

[1] Abogado (UBA). Especialista en Administración de Justicia (UBA). Especializado en Derecho Informático (CEDI-UBA). Graduado del Programa Argentino de Capacitación para la Reforma Procesal Penal (CEJA-INECIP). Formación de posgrado en Análisis Económico del Derecho y en Género, Sexualidad y Diversidad (Escuela Complutense Latinoamericana. Docente por concurso de oposición y antecedentes del Departamento de Derecho Penal de la Facultad de Derecho de la Universidad de Buenos Aires (UBA). Docente de posgrado en el Programa de Actualización en Ciberseguridad y Delitos Informáticos (UBA) y en el Diploma en Cibercrimen de la Universidad Nacional de Quilmes (UNQUI). Ex cotitular de la Dirección General de Capacitación y Escuela del Ministerio Público Fiscal de la Nación. Asesor de la Comisión para la Reforma del Código Penal. Subsecretario letrado de la Procuración General de la Nación. Asesor de la Comisión para la Reforma del Código Penal (creada por Decreto PEN 103/2017). Ganador del Primer premio en el Concurso de Investigaciones de Derecho Penal Económico - Instituto Transdisciplinario de Estudios Penales de América del Sur -ITEP Sur- (2018). Premio "mención académica" - Rectorado UBA (2019). Conferenciante y formador en Red de Capacitación del Ministerio Público Iberoamericano, H. Senado de la Nación, Ministerio Público Fiscal de la Nación, entre otros. Codirector de la revista "Temas de Derecho Penal y Procesal Penal" (ed. Erreius). Coautor de los libros "Delitos Tributarios y contra la Seguridad Social", Rubinzal Culzoni (2020), "El delito de contrabando", Rubinzal Culzoni, Santa Fe, (2017), "Desafíos y tensiones creativas de la reforma procesal penal", Al Sur, Buenos Aires (2015) y "Derecho Penal Económico", Marcial Pons, Buenos Aires (2010).

Penal; III.- Algunas consideraciones finales; IV.- Anexo comparativo entre el Código Penal argentino y el proyecto de nuevo Código Penal en materia de delitos informáticos vigentes

RESUMEN: Los delitos informáticos se encuentran en un proceso de expansión que se ha visto favorecido por la rápida y constante evolución de las tecnologías de la información y la comunicación. La pandemia de Covid-19 ha facilitado aún más su proliferación. Mediante este artículo se procurara elaborar un panorama sobre el modo en que los delitos informáticos se encuentran regulados en la Argentina. También se brindaran ciertas notas de actualidad a su respecto, enmarcadas en el contexto sanitario anteriormente aludido. Asimismo se expondrán las propuestas de cambio que el proyecto de nuevo Código Penal argentino ha contemplado para este tipo de manifestaciones delictivas. Finalmente se esbozaran ciertas conclusiones derivadas de la comparación entre la legislación vigente y la proyectada.

PALABRAS CLAVE: delitos informáticos – cibercrimen – proyecto de nuevo Código Penal argentino – delitos en pandemia – tecnologías de la información y la comunicación

I.- Introducción

A poco más de dos años de desatada la pandemia mundial de Covid-19 la especie humana sigue atravesándola y lidiando con transformaciones del más diverso tipo. Son cambios que han alterado la previsibilidad de nuestro ritmo de vida a nivel global y que a muchas personas nos tienen expectantes, en procura de poder proyectarnos racionalmente a futuro en aspectos múltiples (relacional, profesional, laboral, educacional, comercial, etc.), tanto en lo individual como en lo colectivo, que hacen a nuestro plan de vida.

Todo este dinámico escenario se nutre de factores coyunturales (por ej., los condicionamientos que impone cada nueva cepa del Covid-19, los alcances de las campañas de vacunación, entre otros) que se conjugan con bagajes y proyecciones preexistentes, para dar lugar así al marco de la –no poco cuestionada– noción de *nueva normalidad*.

En este contexto ha sido fundamental el rol que las tecnologías de la información y la comunicación (TIC) e internet han desempeñado y que han redundado en un beneficio a la hora de que nuestras existencias no se vean

mayormente afectadas en una época de tanta zozobra[2], cuya contracara (o *lado "B"*) vino dada por la paralela proliferación de un amplio abanico de nuevos riesgos para la sociedad, entre ellos, la generación de ambientes mayormente propicios para una creciente perpetración de delitos informáticos y de conductas *ciber* que, aunque no estén contempladas por la ley penal, igualmente afectan bienes jurídicos de relevancia con suficiente contundencia.

En la Argentina una parte de dichas manifestaciones resulta de susceptible abordaje por el sistema de administración de justicia en materia penal, dado que existen herramientas normativas suficientes para su tratamiento, desde que en 2008 se sancionó la *ley de delitos informáticos* (N° 26.388), mediante la cual introdujeron diversas reformas al Código Penal, para que quedase en condiciones de ofrecer alternativas ante ese tipo de comportamientos criminales. Sin embargo, no puede perderse de vista que desde aquel entonces se han suscitado numerosos adelantos tecnológicos y comunicacionales que justifican pensar si las figuras incorporadas mediante aquella legislación son actualmente suficientes como para brindar las respuestas adecuadas desde el ámbito que concierne al Derecho penal. A su vez, el 25 de marzo de 2019 se presentó ante el Senado de la Nación un proyecto de ley que busca actualizar y armonizar integralmente el Código Penal argentino[3] (cuya existencia data ya de 100 años, lapso en el cual ha sufrido diversas modificaciones que han mermado su sistematicidad[4]), el cual contiene innovadoras propuestas en materia de delitos informáticos.

---

[2] Pensemos tan solo en cómo múltiples sectores de la población se ha valido de la telemedicina, el teletrabajo, la teleeducación y el comercio electrónico –con la incursión de nuevas modalidades de pago y la proliferación de los criptoactivos– en pos de seguir adelante con sus vidas, aún bajo la incidencia del padecimiento sanitario

[3] El proyecto de reforma del Código Penal argentino fue elaborado por la comisión creada mediante el Decreto 103/17, la cual fue presidida por el camarista federal de la Casación Penal, Mariano H. Borinsky, acompañado por un conjunto de juristas conformado por Carlos M. González Guerra, Pablo N. Turano, Carlos A. Mahiques, Patricia M. Llerena, Pablo López Viñals, Guillermo J. Yacobucci, Fernando J. Córdoba, Patricia S. Ziffer, Yael Bendel y Guillermo Soares Gache. Su texto se encuentra publicado en https://www.argentina.gob.ar/sites/default/files/proyecto_de_ley_-_reforma_del_codigo_penal.pdf y sus fundamentos en https://www.senado.gob.ar/upload/29740.pdf (ambos textos consultados por última vez el 22/12/2021).

[4] El Código Penal argentino fue sancionado en 1921 y modificado por más de 900 leyes, sin tener en cuenta la sistematicidad de la totalidad de los institutos, de las reglas generales y de los delitos contemplados. También ha ido incorporando todas las leyes penales especiales. De esta

Sobre la base de lo antedicho, en lo que sigue procuraremos trazar un sobrevuelo en relación a la legislación vigente en Argentina en materia de delitos informáticos, contrastarla con las propuestas del *proyecto de nuevo Código Penal* y mechar ese cotejo con datos de actualidad en materia de cibercrimen, fundamentalmente en función de los cambios que ha aparejado la pandemia del Covid-19. Procuraremos luego trazar algunas conclusiones.

II.- Legislación argentina vigente en materia de delitos informáticos y propuestas de actualización mediante el proyecto de nuevo Código Penal

II.A.- Delitos informáticos contra la integridad sexual

II.A.1.- Producción, financiación, ofrecimiento, comercialización, publicación, facilitación, divulgación y distribución de imágenes de abuso sexual infantil. Su tenencia simple y con fines de comercialización.

El artículo 128 del Código Penal fue, dentro de su parte especial, el primero que resultó reformado por la *ley de delitos informáticos*. Posteriormente, en 2018, aquella disposición fue objeto de un nuevo cambio por medio de la ley 27.436[5].

manera, perdió su coherencia interna y la proporcionalidad que le son esenciales, y se apartó del criterio de codificación unificada en materia penal.

[5] Producto de ambas modificaciones el art. 128 CP quedó redactado de la siguiente manera:

- 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.

En esencia, en lo que aquí es de nuestro interés, en su redacción actual la norma contempla la posibilidad de aplicar prisión de 3 a 6 años a quien produzca, financie, ofrezca, comercie, publique, facilite, divulgue o distribuya, a través de los nuevos medios electrónicos (internet), toda representación de un menor de dieciocho años dedicado a actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales.

También prevé prisión de 4 meses a 1 año para quien, con conocimiento, incurriere en la mera tenencia de representaciones como las evocadas. La pena se eleva a prisión de 6 meses a 2 años si esa tenencia tuviese fines inequívocos de distribución o comercialización.

Todas las escalas penales referenciadas se incrementan en un tercio en su mínimo y en su máximo en caso de que la víctima fuere menor de 13 años.

De ese modo, se apunta a brindar una protección al derecho de personas menores de edad a no ser utilizadas en producciones, publicaciones o espectáculos que pongan en peligro el normal desarrollo de su personalidad, psiquis y conducta sexual.

Distintos instrumentos internacionales han incidido en la tipificación de las figuras aludidas, entre ellos la Convención de los Derechos del Niño[6] (que en Argentina goza de jerarquía constitucional), el Protocolo Facultativo de la Convención sobre los Derechos del Niño Relativo a la Venta de Niños, la Prostitución Infantil y la Utilización de Niños en la Pornografía[7] y el Convenio sobre la cibercriminalidad de Budapest[8]. Este último alude en su artículo 9 a los *delitos relacionados con la pornografía infantil*, terminología que se encuentra severamente cuestionada desde hace algún tiempo, dado que la *pornografía* es un término utilizado para adultos que realizan actos sexuales consentidos y distribuidos casi siempre de forma lícita al público en general para su disfrute sexual, lo cual nada tiene que ver con el abuso sexual infantil[9].

Según datos de la Línea 137 para víctimas de violencia sexual o familiar del Ministerio de Justicia y Derechos Humanos de la Nación, el total de violencias en

[6] Arts. 1 y 34.

[7] Arts. 2 y 3.

[8] Título 3.

[99]En ese sentido se ha expresado, por ej. Interpol en https://www.interpol.int/es/Delitos/Delitos-contra-menores/Terminologia-apropiada (consultado por última vez el 22/12/2021).

entornos digitales aumentó, durante el 20 de marzo y el 20 de septiembre de 2020, un 195,3% respecto al mismo período de 2019. La utilización de niños, niñas y adolescentes en imágenes de abuso sexual se disparó un 522,5%[10].

El *proyecto de nuevo Código Penal* –en esencia– recepta sin alteraciones las conductas hoy día acuñadas en el art. 128 CP, pero incrementa el mínimo de la penal a cuatro años de prisión si el autor actuare con fines de lucro[11]. Asimismo, prevé como agravante que eleva mínimos y máximos en un tercio no solo el hecho de que la víctima sea menor de trece años (tal como en la actualidad se encuentra previsto), sino además la circunstancia de que el material registrado represente especial violencia física contra la víctima y la comisión del hecho por parte de un ascendiente, afín en línea recta, hermano, tutor, curador, ministro de algún culto reconocido o no, encargado de la educación o de la guarda[12].

II.a.2.- Ciber acoso sexual a personas menores de edad (grooming)

Grooming es un término de la lengua inglesa (un anglicismo) que proviene del vocablo *groom*, que significa acicalar, preparar, asear, cuidar. Ello nos habla de la modalidad de pedófilos y pederastas, quienes cuidadosamente dirigen sus acciones con la intención de crear una conexión emocional con niños, niñas y adolescentes para reducir sus inhibiciones y poder abusar sexualmente ellos.

En Argentina el artículo 131 CP es la disposición que se ocupa de reprimir con prisión de 6 meses a 4 años a quien, por medio de comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos, tomare contacto con una persona menor de edad, con el propósito de cometer cualquier delito contra su integridad sexual[13].

Se trata de un *delito informático impropio*, en la medida que la informática es utilizada como medio para la comisión del delito, en contraposición de los

[10] Durante la pandemia, la utilización de menores en pornografía creció más del 500% en Argentina, diario Infobae del 4/9/2021, disponible en https://www.infobae.com/sociedad/2021/09/04/durante-la-pandemia-la-utilizacion-de-menores-en-pornografia-crecio-mas-del-500-en-argentina/ (consultado por última vez el 22/12/2021).

[11] Proyecto de nuevo Código Penal, art. 123.

[12] Proyecto de nuevo Código Penal, art. 124.

[13] CP, art 131: 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.

llamados *delitos informáticos propios*, que son aquellos en donde el objeto de protección se vincula con los datos informáticos a los que se accede mediando falta de la debida autorización o manipulando la seguridad.

La inclusión de esta figura en el Código Penal argentino no tuvo lugar por medio de la *ley de delitos informáticos* (N° 26.388), sino mediante una normativa específica: la ley 26.904 de 2013. Si bien el Convenio de Budapest no consagra el delito en cuestión, el instrumento internacional que mayor incidencia ha tenido para que en Argentina se tipifique el *grooming* es el Convenio de Lanzarote para la Protección de los Niños Contra la Explotación y el Abuso Sexual del Consejo de Europa[14]. La Convención sobre los Derechos del Niño es otro plexo normativo que ha tallado decididamente en la contemplación del art. 131 CP.

Tal como sintetiza Riquert[15], el *proyecto de nuevo Código Penal* pune el *grooming* tanto cuando: *a)* se limita a la mera puesta en contacto mediante conversaciones o relatos de contenido sexual; *b)* se requiera la realización de actividades de connotación sexual o toma de imágenes de aquellas; *c)* se proponga un encuentro para la práctica de actividades sexuales[16]. En todos los casos, el sujeto activo es una persona mayor y el sujeto pasivo una de menor de 13 años, con lo cual se refinaría la técnica legislativa vigente en cuanto concierne a la franja etaria de victimarios y víctimas (aspecto carente de limitaciones en el art. 131 CP). Además, la iniciativa es superadora de una de las grandes críticas que actualmente recibe el tipo penal de *grooming*, al ampliarlo hacia cualquier medio comisivo, con lo cual ya no quedaría supeditado a la mediación de la tecnología de transmisión de datos (dicho en términos llanos, sería posible la comisión del *grooming* presencial, perpetrado *cara a cara*). También prevé una escala penal más grave, con una pena máxima de 5 años de prisión.

II.b.- Delitos informáticos contra la libertad

II.b.1.- Acceso ilegítimo a un sistema o dato informático

No ya una reforma de una pretérita disposición, sino toda una novedad resultó la incorporación que la *ley de delitos informáticos* efectuó al Código Penal al

[14] Argentina no ha suscripto el tratado referenciado, pero aún así su incidencia ha sido decisiva a la hora de motivar la previsión normativa del *grooming* como delito contra la integridad sexual.

[15] Riquert, Marcelo A., *Delitos informáticos en el anteproyecto de Código Penal de 2018*, disponible en http://www.pensamientopenal.com.ar/doctrina/47358-delitos-informaticos-anteproyecto-codigo-penal-2018 (consultado por última vez el 22/12/2021).

[16] Proyecto de nuevo Código Penal, art. 122.

introducir su art. 153 bis[17], mediante el cual –residualmente– se prevé la posibilidad de aplicar prisión de 15 días a 6 meses a quien, a sabiendas, accediere por cualquier medio, sin autorización o en exceso de la existente, a un sistema o dato informático de acceso restringido. La sanción pasa a ser de 1 mes a 1 año de prisión si el acceso se efectúa 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 ello quedó cubierta la exigencia del Convenio de Budapest, en cuanto prevé que las partes deben tipificar penalmente el acceso doloso y sin autorización a todo o parte de un sistema informático. El instrumento faculta a que los signatarios puedan contemplar que la infracción sea cometida con vulneración de medidas de seguridad, con la intención de obtener los datos informáticos o con otra intención delictiva, o también requerir que se perpetre en un sistema informático conectado a otro sistema informático. Sin embargo, la legislación vigente en Argentina no echó mano a ninguna de tales posibilidades. Con ello la normativa resultante derivó en una expresión mayormente tributaria del fenómeno de la *inflación penal (normativa)*, al amparo de una salvaguarda de la intimidad que, si bien reconoce anclaje constitucional[18], podría haber reconocido límites más afines al principio de subsidiariedad y de última ratio del Derecho penal.

Como dato de actualidad puede señalarse que entre abril de 2019 y marzo de 2020 la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público Fiscal de la Nación (Argentina) detectó 229 casos de acceso ilegítimo a sistemas o datos informáticos, mientras que en los doce meses posteriores –es decir en plena pandemia del Covid-19– se relevaron 1.220 maniobras (la cantidad de casos se quintuplicó)[19].

---

[17] CP, art. 153 bis: 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.

[18] Constitución Nacional, arts. 18 y 19; Convención Americana de Derechos Humanos, art. 11; Pacto Internacional de Derechos Civiles y Políticos, art. 17.

[19] Informe de gestión 2020 de la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público Fiscal de la Nación –Argentina–, disponible en https://www.fiscales.gob.ar/wp-content/uploads/2021/09/UFECI_informe-pandemia.pdf , consultado por última vez el 22/12/2021).

El *proyecto de nuevo Código Penal* tomó sin mayores cambios el tipo penal del artículo 153 bis CP en su artículo 501, el cual quedó alojado en el segmento específico dedicado a la rúbrica de los "Delitos Informáticos"[20]. La pena se incrementa a un mínimo de 6 meses a 2 años de prisión cuando por su forma de comisión el delito afecte a un número indiscriminado de víctimas o 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 salud o financieros[21]. A su vez se agrava doblemente la pena cuando se viere afectada información sensible a la defensa nacional, supuesto en el que el máximo de prisión se eleva a 4 años.

II.b.2.- Acceso, apoderamiento, supresión o desvío de comunicación electrónica. Comunicación o publicación de su contenido

Los cambios que la *ley de delitos informáticos* introdujo en el artículo 153 del Código Penal argentino[22] habilitaron la punición con prisión de 15 días a 6 meses para quien fuera más allá de un mero acceso ilegítimo y: *a)* accediere indebidamente a una comunicación electrónica que no le esté dirigida; *b)* se apoderare indebidamente de tal tipo de misiva; *c)* indebidamente suprimiere o desviare de su destino una comunicación electrónica que no le esté dirigida; *d)* indebidamente interceptare o captare comunicaciones electrónicas. La disposición duplica la escala penal para el sujeto activo que, además, comunicare a otro o publicare el contenido de la comunicación electrónica. Asimismo, contempla la inhabilitación especial por el doble del tiempo de la condena si el hecho lo cometiere un funcionario público que abusare de sus funciones.

---

[20] Libro Segundo, Título XXVI.

[21] Proyecto de nuevo Código Penal, art. 502.

[22] CP, art. 153: 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.

La disposición se emparenta con el art. 3 del Convenio de Budapest, que exige a las partes tipificar penalmente la interceptación, dolosa y sin autorización, cometida a través de medios técnicos, de datos informáticos –en transmisiones no públicas– en el destino, origen o en el interior de un sistema informático, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporta tales datos informáticos.

En su art. 153 el *proyecto de nuevo Código Penal* propone endurecer notablemente la reacción punitiva al elevar la pena de prisión para la figura básica, que pasaría a ser de 6 meses a 2 años, con añadidura de una pena de 10 a ciento cincuenta 150 días-multa. También aumenta la sanción para la conducta adicional de quien comunica a otro o publica el contenido de la comunicación electrónica ilegítimamente accedida, apoderada, suprimida o desviada, respecto de la cual se prevé un mínimo de 1 año de prisión y un máximo de 3. Esta misma reacción se contempla para quien hiciere publicar ese contenido, conducta que actualmente no se encuentra legislada y que representaría, entonces, una innovación.

II.b.3.- Publicación ilegal o abusiva de comunicaciones

Dentro de la gama de conductas incorporadas al Código Penal por la *ley de delitos informáticos* una de las más levemente penadas la encontramos en el art. 155[23], que prevé multa de $ 1.500[24] pesos a $ 100.000 para quien poseyere una comunicación electrónica no destinada a la publicidad y la hiciere publicar indebidamente, si el hecho causare o pudiere causar perjuicios a terceros; a menos que hubiere obrado con el propósito inequívoco de proteger un interés público, en cuyo caso está exento de responsabilidad penal.

En lo que para nosotros aquí es de interés, el *proyecto de nuevo Código Penal* prácticamente reproduce el contenido del actual artículo 155 CP en su artículo 154,

[23] CP, art. 155: 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.
Está exento de responsabilidad penal el que hubiere obrado con el propósito inequívoco de proteger un interés público.

[24] Téngase en cuenta, para tener un parámetro internacional, que el dólar oficial promedio para la compra en Argentina cotiza a $ 101.90 la unidad, y para la venta $109.10; mientras que el dólar paralelo o informal cotiza para la compra a $ 201,50 y para la venta a $203,50 (valores al 27/12/2021).

con el agregado de que el interés público salvaguardado que da pie a la excusa absolutoria acuñada por la normativa debe revestir carácter "actual", lo cual otorga mayor precisión a los límites de la disposición. Asimismo, busca reemplazar la pena de multa actual por prisión de 6 meses a 2 años.

II.b.4.- Revelación de secretos oficiales

El artículo 157 CP[25] también fue objeto de reforma por parte de la *ley de delitos informáticos*, gracias a lo cual es hoy día pasible de ser penado con prisión de 1 mes a 2 años e inhabilitación especial de 1 a 4 años, el funcionario público que revelare documentos (informáticos)[26] o datos que por ley deben ser secretos.

Este delito especial propio encuentra su correlato en el art. 156 del *proyecto de nuevo Código Penal*, que lo emula, aunque contempla una elevación de la reacción punitiva, que se propone que vaya de los 6 meses a los 2 años de prisión e inhabilitación especial por doble del tiempo de la condena a la pena privativa de la libertad.

II.b.5.- Acceso ilegítimo a banco de datos personales, revelación ilegítima de su información e inserción ilegítima de datos

Otra de las reformas introducidas por la *ley de delitos informáticos* impactó en el artículo 157 bis del Código Penal[27], en función del cual es pasible de ser penado con prisión de 1 mes a 2 quien ingrese a un banco de datos personales sin autorización ni permiso alguno; quien revelare secretos o archivos registrados en

[25] CP, art. 157: 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.

[26] Para la legislación argentina el término "documento" comprende toda representación de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión (CP, art. 77, el cual también fue reformado, para que tuviera un alcance acompasado con los avances tecnológicos, por la *ley de delitos informáticos*).

[27] CP, art. 157 bis: 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;
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 (1) a cuatro (4) años.

ese banco de datos y quien los modifique por cualquier medio. Se añade la pena de inhabilitación especial de 1 a 4 años si el sujeto activo es un funcionario público.

Esta figura, que se asocia con la privacidad (entendida como bien jurídico susceptible de ser desdoblado en dos facetas: *a.* como prerrogativa excluyente de terceros respecto de determinados ámbitos de la vida privada y *b.* como derecho de control sobre la información y los datos de la propia persona, incluso los ya conocidos, para que solo puedan usarse según la voluntad de su titular) es reproducida por el art. 157 del *proyecto de nuevo Código Penal*, el cual añade la conducta de supresión ilegítima de datos en un archivo de datos personales. Las penas también son objeto de aumento en el marco de la propuesta, en la medida que la prisión contemplada por na norma proyectada va de 6 meses a 2 años, mientras que si el autor fuere funcionario público, se prevé la adicional imposición de inhabilitación de 1 a 5 años.

II.c.- Delitos informáticos contra la propiedad

II.c.1.- Estafa mediante el uso de tarjeta magnética o sus datos

Previo a la sanción, promulgación y entrada en vigencia de la *ley de delitos informáticos* el Código Penal argentino ya había sido reformado en 2004 por la ley 25.930, en función de la cual el artículo 173 inciso 15[28] de aquel plexo normativo pasó a contemplar como punible con prisión de 1 mes a 6 años la conducta de quien –en lo que para nosotros aquí es de interés– defraudare mediante el uso no autorizado de los datos de una tarjeta de compra, crédito o débito, aunque lo hiciere por medio de una operación automática.

Esa modificación procuró atender a un aspecto de la protección del patrimonio que hasta ese entonces se encontraba inserto en una laguna normativa, en función de avances tecnológicos cuyos alcances se han multiplicado

[28] CP, art. 173: sin perjuicio de la disposición general del artículo precedente, se considerarán casos especiales de defraudación y sufrirán la pena que él establece (prisión de un mes a seis años):

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.

exponencialmente hasta la actualidad, en función del auge de las compras en línea, basadas en el empleo de datos vinculados a las tarjetas de referencia[29].

La disposición se mantiene sin cambios dentro del *proyecto de nuevo Código Penal*, donde incluso ha mantenido la misma numeración en lo que al articulado se refiere.

II.c.2.- Defraudación informática

Sí fue gracias a la ley de delitos informáticos que el Código Penal pasó a contar con una disposición específica mediante la cual se previó como conducta punible, con prisión de 1 mes a 6 años, la defraudación mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos (artículo 173 inciso 16).

El convenio de Budapest manda a que las partes tipifiquen penalmente la *estafa informática*, entendida como la producción de un perjuicio patrimonial a otro, de forma dolosa y sin autorización, a través de la introducción, alteración, borrado o supresión de datos informáticos, o mediante cualquier forma de atentado al funcionamiento de un sistema informático, con la intención, fraudulenta o delictiva, de obtener sin autorización un beneficio económico para sí mismo o para un tercero[30].

El actual inciso 16 del artículo 173 del Código Penal argentino es trasladado art. 500 del *proyecto de nuevo Código Penal* (dentro del Título XXVI, especialmente dedicado a los delitos informáticos). Sin embargo, la redacción propuesta reconoce un refinamiento de técnica legislativa, ya que diferencia entre el fraude informático que puede cometerse alterando los datos de un sistema de aquel que es susceptible de ser perpetrado mediante la alteración de programas que alteran el funcionamiento del sistema (situaciones diferenciadas que en la actual letra del CP aparecen confundidas).

[29] Según el Banco Central de la República Argentina, durante 2020 se registró un 19% más de operaciones por medios electrónicos que en el 2019, mientras que las transferencias electrónicas se acrecentaron en un 90%, producto de un aumento en las operaciones por medio de *homebanking* (86%) y *mobilebanking* (167%). A su vez, los pagos remotos con tarjeta de débito crecieron en un 227% (guarismos extraídos del Informe de gestión 2020 de la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público Fiscal de la Nación –Argentina–, disponible en https://www.fiscales.gob.ar/wp-content/uploads/2021/09/UFECI_informe-pandemia.pdf, consultado por última vez el 22/12/2021).

[30] Convenio de Budapest, art. 8.

Como dato de actualidad puede señalarse que según la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público Fiscal de la Nación (Argentina), durante abril de 2019 y marzo de 2020 los casos de fraude en línea ascendieron a un total de 1.305, mientras que los fraudes *on line* detectados entre abril de 2020 y marzo de 2021 ascendieron a 8.559 reportes[31].

II.c.3.- Daño informático

La *ley de delitos informáticos* aggiornó en su momento el Código Penal argentino en materia de daños, al modificarlo de modo tal que el segundo párrafo de su artículo 183[32] previera pena de prisión de 15 días a 1 año para quien alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos, como así también para quien vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa dañino.

También lo hizo al transformar el artículo 184 CP[33], que entre las hipótesis agravadas, que prevén prisión de 3 meses a 4 años, pasó a contemplar la ejecución

[31] Informe de gestión 2020 de la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público Fiscal de la Nación –Argentina–, disponible en https://www.fiscales.gob.ar/wp-content/uploads/2021/09/UFECI_informe-pandemia.pdf (consultado por última vez el 22/12/2021).

[32] CP, art. 183: será reprimido con prisión de quince (15) días a un (1) año el que destruyere, inutilizare, hiciere desaparecer o de cualquier modo dañare una cosa mueble o inmueble o un animal, total o parcialmente ajeno, siempre que el hecho no constituya otro delito más severamente penado

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.

[33] CP, art. 184: la pena será de tres (3) meses a cuatro (4) años de prisión, si mediare cualquiera de las circunstancias siguientes:

1. Ejecutar el hecho con el fin de impedir el libre ejercicio de la autoridad o en venganza de sus determinaciones;
2. Producir infección o contagio en aves u otros animales domésticos;
3. Emplear substancias venenosas o corrosivas;
4. Cometer el delito en despoblado y en banda;
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.

del daño en datos, documentos, programas o sistemas informáticos públicos; como así también su perpetración 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.

Ambas regulaciones se encuentran en estrecha relación con las disposiciones de los arts. 5 y 6 del Convenio de Budapest.

El *proyecto de nuevo Código Penal* acuña el daño informático como figura específica dentro del Título XXVI, referido a los delitos informáticos, en su artículo 494. La pena privativa de la libertad se mantiene incólume con relación a que hoy día se encuentra vigente, pero se conjuga con la alternativa de la pena de días multa, para quien despliegue las mismas conductas que actualmente contempla el art. 183 CP, pero suma la posibilidad de afectar por medio de ellas registros informáticos de cualquier índole.

Se prevé a su vez, un incremento de la escala penal en un tercio del mínimo y del máximo, cuando los datos, documentos o programas afectados sean aquéllos protegidos por la *ley de Confidencialidad sobre la información y productos que estén legítimamente bajo control de una persona y se divulgue indebidamente de manera contraria a los usos comerciales honestos* (N° 24.766).

En cuanto a las agravantes, el art. 495 también mantiene inalterada la pena privativa de la libertad que actualmente contempla el CP en el art. 184, aunque puesta en combinación con la alternativa de los días-multa, para conductas prácticamente análogas a las que alude esta última disposición. Se innova al establecer como adicional agravante el caso de que el hecho recayera sobre un bien perteneciente al patrimonio cultural de la Nación o de un Estado extranjero.

Tres nuevas agravantes, con penas aún más graves, propone incorporar el *proyecto de nuevo Código Penal* en su artículo 496, que dispone que la pena será de 1 a 5 años cuando por la forma de comisión del daño informático haya afectado a un número indiscriminado de sistemas informáticos o hubiera perjudicado el funcionamiento de servicios públicos esenciales o la provisión de bienes de primera necesidad o el daño hubiera creado una situación de peligro grave para la sociedad.

Por su parte, el artículo 497 del *proyecto de nuevo Código Penal* propone reprimir con esa misma escala penal a quien ilegítimamente y sin autorización de su titular mediante cualquier artificio tecnológico, mecanismo de cifrado o programas maliciosos obstaculice o interrumpa el funcionamiento de un sistema informático

ajeno o impida a los legítimos usuarios el acceso a los datos del sistema siempre que el hecho no importe un delito más severamente penado. Esta figura busca incriminar específicamente una conducta que ha ido notable en crecimiento, el denominado secuestro de datos (*ransomware*), que consiste en hacer inaccesibles los datos de un sistema para pedir posteriormente una suma de dinero de cara a la devolución del uso de los datos al titular legítimo[34].

Finalmente, mediante el artículo 498 del *proyecto de nuevo Código Penal* se procura sancionar con prisión 15 días a 1 año quien vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños. Se trata de un supuesto de peligro de daño informático.

II.d.- Delitos informáticos contra la seguridad pública que atentan contra los medios de comunicación

II.d.1.- Entorpecimiento de comunicaciones electrónicas y resistencia a su restablecimiento

El artículo 197 del Código Penal[35] argentino pasó a considerar la aplicación de prisión de 6 meses a 2 años para quien interrumpiere o entorpeciere la comunicación electrónica o resistiere violentamente el restablecimiento de la

[34] Como dato de actualidad puede evocarse que durante el periodo de pandemia motivado en el Covid-19 la Unidad Fiscal Especializada en Ciberdelincuencia advirtió un aumento en la cantidad de maniobras de *ransomware* reportadas. Durante los doce meses previos a la pandemia, los casos reportados fueron 10, mientras que, para el año siguiente, el número ascendió a 38, lo que significa que el aumento fue de aproximadamente 280% (Informe de gestión 2020 de la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público Fiscal de la Nación –Argentina–, disponible en https://www.fiscales.gob.ar/wp-content/uploads/2021/09/UFECI_informe-pandemia.pdf, consultado por última vez el 22/12/2021). También se ha señalado que durante el transcurso de la pandemia se produjo un notable incremento de estos ataques a nivel de organizaciones que tuvieron como objetivo fundamentalmente al sector privado, donde los blancos principales fueron grandes empresas, esencialmente por la capacidad adquisitiva para pagar las millonarias sumas demandadas (Sain, Gustavo, *Nuevas modalidades delictivas en materia de cibercrimen durante la pandemia del Covid-19 en la República Argentina*, publicado en Borinsky, Mariano H. y Schurjin Almenar, Daniel [directores], revista "Temas de Derecho Penal y Procesal Penal", Erreius, Buenos Aires, ejemplar Diciembre-2021, pp. 1295/1302).

[35] CP, art. 197: 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.

comunicación electrónica interrumpida, gracias a la reforma de provocada por la *ley de delitos informáticos*.

El *proyecto de nuevo Código Penal* busca elevar la reacción punitiva al promover que se aplique prisión de 6 meses a 3 años para quien, aun sin crear un peligro común, ejecutare cualquier acto tendiente a interrumpir o entorpecer el funcionamiento de los servicios públicos de comunicación electrónica o resistiere con violencia su restablecimiento (art. 192).

II.e.- Delitos informáticos contra la administración pública

II.e.1.- Violación de pruebas, registros y documentos electrónicos

En el terreno de los delitos que se enfocan sobre bienes jurídicos supraindividuales, la *ley de delitos informáticos* talló el artículo 255 del Código Penal argentino[36], de manera tal que allí quedó legislada la conducta de quien sustrajere, alterare, ocultare, destruyere o inutilizare en todo o en parte, registros o documentos electrónicos confiados a la custodia de un funcionario público o de otra persona en el interés del servicio público, para la cual se prevé prisión de 1 mes a 4 años, salvo que el autor fuere el mismo depositario, en cuyo caso sufrirá además inhabilitación especial por doble tiempo; o que el hecho se cometiere por imprudencia o negligencia del depositario, quien –en ese caso– será reprimido con multa de $ 750 a $ 12.500.

La contemplación de estas conductas delictivas se mantuvo sin cambios en el *proyecto de nuevo Código Penal*, aunque con aumento el mínimo de la escala penal, que pasaría a ser de 6 meses y con remplazo del monto de la multa por los correspondientes días-multa (art. 255).

II.f.- Otros delitos informáticos propuestos por el proyecto de nuevo Código Penal argentino

Hasta aquí hemos hecho, principalmente, un repaso por las figuras que el Código Penal argentino ha receptado en materia de criminalidad informática en

[36] CP, art. 255: 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).

función de las reformas introducidas por la *ley de delitos informáticos* (N° 26.388), sumadas otras expresiones que se incorporaron a aquel plexo normativo con motivo las reformas promovidas por distintas leyes. Asimismo, realizamos una correlación con las disposiciones que al respeto contempla el *proyecto de nuevo Código Penal*, iniciativa que prevé adicionales tipos penales en materia de delitos informáticos que actualmente no se encuentran acuñados en el ordenamiento jurídico de la Argentina. Las repasaremos en lo sucesivo.

II.f.1.- Obtención de datos personales de la víctima mediante engaños (phishing[37] - pharming[38])

El artículo 491 del *proyecto de nuevo Código Penal*[39] busca reprimir la obtención ilegítima de datos personales de la víctima mediante técnicas de ingeniería social o manipulaciones informáticas como el *pharming*.

Con elocuencia se explicita en los fundamentes del proyecto que "Estas quedan abarcadas por el Código Penal vigente recién cuando los datos son utilizados para la comisión de un delito más grave (por ejemplo, fraude) que en la mayoría de los supuestos son cometidos por autores diferentes a quien obtuvo y vendió o distribuyó de alguna manera los datos, lo que genera problemas para su persecución como delito autónomo. Significa adelantar la punición a las conductas descriptas sin perjuicio de que algunos supuestos queden subsumidos por un delito más grave. O sea, punir la mera obtención ilegítima de los datos o su venta y compilación con independencia del delito más grave en el que pueden ser utilizados, muy probablemente por otros autores".

[37] El término deriva de expresión *password harvesting fishing* (cosecha y pesca de contraseñas).

[38] El *pharming* consiste en dotar de ciertos ropajes a sitios web falsos, como si fueran auténticos (en lo que se denomina su *look and feel)*, para obtener así la información que se introduzca en ellos.

[39] *Proyecto de nuevo Código Penal*, art. 491: 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.

La misma pena se impondrá a quien compilare, vendiere, intercambiare u ofreciere, de cualquier manera, claves o datos de los mencionados en el primer párrafo.

La pena será de prisión de uno (1) a tres (3) años, en cualquiera de los casos de este artículo, cuando se tratare de un organismo público estatal.

Como dato de actualidad puede referirse que a partir del *aislamiento social preventivo y obligatorio* decretado por el gobierno durante marzo de 2020[40], se notó un incremento de modalidades fraudulentas a través de cuentas falsas de bancos creadas por los *phishers* en redes sociales, sobre la base de un aumento de vías de contacto web establecidos por las instituciones bancarias a partir del trabajo remoto de muchos de sus clientes y el aforo temporal en la atención personalizada en las sucursales. En relación a este tipo de engaños, durante la pandemia, pasaron a constatarse amenazas direccionadas (personalizadas), a partir de datos correspondientes a las víctimas en concreto, previamente obtenidos, modalidad se denomina *spearphishing*[41].

II.f.2.- Sustitución de identidad digital destinada a la comisión de un delito o a causar perjuicio

Una de las problemáticas asociadas a la protección de datos que más recibió el Centro de Ciberseguridad del Gobierno de la Ciudad de Buenos Aires es la de la suplantación de identidad. Durante 2020, se reportaron 102 incidentes de este tipo[42].

El artículo 492 del *proyecto de nuevo Código Penal*[43] procura acuñar la suplantación de identidad digital con la intención de cometer un delito o causar un perjuicio a la persona cuya identidad se suplanta o a terceros (es decir mediante la cortapisa de un elemento subjetivo distinto del dolo) y reprimir ese tipo de conducta con prisión de 6 meses a 2 años de prisión o 6 a 24 días-multa.

---

[40] A partir del 19 de marzo de 2020 el gobierno de la República Argentina decretó el Aislamiento Social Preventivo y Obligatorio en todo el territorio nacional como medida de salud ante la pandemia del Covid-19.

[41] Sain, Gustavo, *Nuevas modalidades delictivas en materia de cibercrimen durante la pandemia del Covid-19 en la República Argentina*, publicado en Borinsky, Mariano H. y Schurjin Almenar, Daniel (directores), revista "Temas de Derecho Penal y Procesal Penal", Erreius, Buenos Aires, ejemplar Diciembre-2021, pp. 1295/1302.

[42] Suplantación de identidad, fraude y robo de cuentas, las modalidades de ciberdelito que más crecieron en CABA, publicado en Infobae el 20/1/2021, disponible en línea en https://www.infobae.com/tecno/2021/01/28/suplantacion-de-identidad-fraude-y-robo-de-cuentas-las-modalidades-de-ciberdelito-que-mas-crecieron-en-caba/ (consultado por última vez el 22/12/2021)

[43] *Proyecto de nuevo Código Penal*, art. 492: Se impondrá prisión de seis (6) meses a dos (2) años o seis (6) a veinticuatro (24) días-multa, 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.

Como adicional dato de actualidad vinculado con este tema cabe tener presente el desarrollo de noticias falsas (*fake news*) o incluso peor, falsificaciones profundas (*deep fakes*) de videos, imágenes o audios de principales jefes de estado mandatarios mediante sofisticados programas de inteligencia artificial (IA) tales como Deep Fake o Lyrebird, que permiten imitar la imagen y el registro de voz de la persona que se desea suplantar con un nivel de realismo y perfeccionamiento que solo son detectables mediante un análisis profesional o mediante el empleo de programas forenses (*Truepic y Seleray*)[44].

II.f.3.- Difusión no autorizada de material de audio y/o imágenes de naturaleza sexual de carácter privado

El fenómeno de la mal llamada *pornografía de venganza* (*revenge porn*)[45] busca ser abordado mediante el artículo 493 el *proyecto de nuevo Código Penal*[46], por el cual se propone la elaboración de un tipo básico mediante el cual se sancione con prisión de 6 meses a 2 años y días multa a quien sin autorización de la persona afectada difunda, revele, envíe distribuya o de cualquier forma ponga a disposición de terceros imágenes, grabaciones de audio o audiovisuales de naturaleza sexual,

[44] Sueiro, Carlos Christian, *La necesidad de incorporar nuevos ciberdelitos al Código Penal de la Nación*, publicado en Borinsky, Mariano H. y Schurjin Almenar, Daniel (directores), revista "Temas de Derecho Penal y Procesal Penal", Erreius, Buenos Ares, septiembre de 2019, pp. 887/918.

[45] El término es cuestionado debido a que llamar *pornografía* a la difusión no consentida de audio y/o imágenes íntimas conlleva dar un permiso tácito para consumir algo que fue creado, o difundido, sin consentimiento. Asimismo, porque utilizar la palabra *venganza* es asumir que las víctimas ocasionaron primero algún daño por lo cual le deben una retribución al perpetrador. Otra razón pasa por lo equívoca que es la expresión puesta en tela de juicio, mediante la cual se pretende aludir a distintas conductas que son perfectamente diferenciables (Maddoks, Sophie, *"Mi vida no es tu peli porno": 5 razones para no usar el término "pornovenganza*", disponible en https://www.genderit.org/es/feminist-talk/mi-vida-no-es-tu-peli-porno-5-razones-para-no-usar-el-termino-pornovenganza, consultado por última vez el 22/12/2021)

[46] *Proyecto de nuevo Código Penal*, art. 493: Se impondrá prisión de seis (6) meses a dos (2) años o seis (6) a veinticuatro (24) días-multa, al que sin autorización de la persona afectada difundiere, revelare, enviare, distribuyere o de cualquier otro modo pusiere a disposición de terceros imágenes o grabaciones de audio o audiovisuales de naturaleza sexual, producidas en un ámbito de intimidad, que el autor hubiera recibido u obtenido con el consentimiento de la persona afectada, si la divulgación menoscabare gravemente su privacidad.

La pena será de prisión de uno (1) a tres (3) años:

1. Si el hecho se cometiere por persona que esté o haya estado unida a la víctima por matrimonio, unión convivencial o similar relación de afectividad, aun sin convivencia.
2. Si la persona afectada fuere una persona menor de edad.
3. Si el hecho se cometiere con fin de lucro.

producidas en un ámbito de intimidad, que el autor hubiera recibido u obtenido con el consentimiento de la víctima, cuando la divulgación menoscabe gravemente su privacidad.

Por otra parte, se prevén agravantes, reprimidas con pena de 1 a 3 años de prisión, cuando los hechos hubieran sido cometidos por persona que esté o haya estado unida a la víctima por matrimonio o análoga relación de afectividad, aún sin convivencia, la víctima fuera menor de edad, o los hechos se hubieran cometido con fin de lucro.

Como dato de actualidad cabe referir que la Unidad Fiscal Especializada en Ciberdelincuencia recibió 106 reportes vinculados a este tipo de ataques entre abril de 2019 y marzo de 2020, mientras que en el año posterior se reportaron 395 casos, lo cual representa un incremento de casos informados del 272,6%[47].

II.f.4.- Hurto de datos informáticos

El *proyecto de nuevo Código Penal* prevé la imposición de la pena de prisión de 1 mes a 2 años a quien viole medidas de seguridad e ilegítimamente se apoderare o copie información contenida en dispositivos o sistemas informáticos ajenos que no esté disponible públicamente y que tengan valor comercial para su titular o para terceros (artículo 499[48]).

II.f.5.- Agravante genérica para los delitos informáticos basada en la calidad de funcionario público del sujeto activo

Para todas las figuras previstas bajo la rúbrica "Delitos Informáticos" en el Título XXVI del *proyecto de nuevo Código Penal*, el art. 503[49] propone la aplicación de una inhabilitación especial por el doble tiempo de la condena, de verificarse que hubiere tenido intervención en los hechos un funcionario público.

[47] Informe de gestión 2020 de la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público Fiscal de la Nación –Argentina–, disponible en https://www.fiscales.gob.ar/wp-content/uploads/2021/09/UFECI_informe-pandemia.pdf (consultado por última vez el 22/12/2021)

[48] *Proyecto de nuevo Código Penal*, art. 499: 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.

[49] *Proyecto de nuevo Código Penal*, art. 503: se establece la pena de inhabilitación especial por el doble tiempo de la condena para el funcionario público que hubiere tenido intervención en estos hechos.

III.- Algunas consideraciones finales

En sí la lista de delitos informáticos que contempla el *proyecto de nuevo Código Penal*, podría seguir ampliándose, ya que contiene figuras que no son un correlato de cuanto se previó mediante la *ley de delitos informáticos* (N° 26.388) y que se encuentran alojadas por fuera del Título XXVI que aquel plexo dedica a las referidas expresiones de criminalidad[50].

Hay algunas conclusiones que podemos extraer de cuanto hemos sobrevolado. La primera de ellas pasa por advertir que no hay delito informático alguno, de los que hoy día están vigentes en la Argentina, que pueda verse despenalizado de llegar a traducirse en derecho positivo el *proyecto de nuevo Código Penal*, en los términos en que fue presentado al Poder Legislativo nacional. Todas las figuras que introdujo en el ordenamiento normativo la *ley de delitos informáticos* tienen su correlato en la iniciativa de reforma que se encuentra a estudio de la Cámara de Senadores, al igual que otros tipos penales que fueron acuñados en el Código Penal mediante reformas practicadas a través de otras leyes.

Por otra parte, en términos generales, puede apuntarse que en las correlaciones referenciadas se evidencia que el *proyecto de nuevo Código Penal*, cuanto menos, mantiene las escalas penales que hoy día contemplan las figuras que forman

[50] Como ejemplo, podemos ver el artículo 504 inciso 8 del *proyecto de nuevo Código Penal* (dentro del Título XXVII - Delitos contra la Propiedad Intelectual), por el cual se prevé la imposición de 3 meses a 6 años o 2 a 72 días-multa, al que con ánimo de obtener un beneficio económico, directo o indirecto, y sin la autorización previa y expresa del titular de los derechos pusiere a disposición del público obras, interpretaciones, fonogramas o emisiones de organismos de radiodifusión a través de un sistema informático, o las almacenare, efectuare hospedaje de contenidos, los reprodujere o distribuyere. La misma pena se establece para el proveedor de servicios de internet que, teniendo conocimiento efectivo de la falta de autorización, continuare permitiendo el uso de su sistema informático para la comisión de las conductas descriptas en este inciso.

Otra muestra la encontramos en el art. 350 del *proyecto de nuevo Código Penal* (dentro del Título XVI – Delitos Fiscales), por el cual se contempla la imposición de prisión de 2 a 6 años, al que de cualquier modo sustrajere, suprimiere, ocultare, adulterare, modificare o inutilizare: 1°) Los registros o soportes documentales o informáticos del fisco nacional, provincial o de la Ciudad Autónoma de Buenos Aires, relativos a las obligaciones tributarias o de los recursos de la seguridad social, con el propósito de disimular la real situación fiscal de un obligado; 2°) Los sistemas informáticos o equipos electrónicos, suministrados, autorizados u homologados por el fisco nacional, provincial o de la Ciudad Autónoma de Buenos Aires, siempre y cuando dicha conducta fuera susceptible de provocar perjuicio y no resulte un delito más severamente penado.

parte del Derecho vigente en la Argentina. En algunos casos las penas se ven aumentadas y en otros se combinan con la posibilidad de aplicación de días-multa, alternativa que resultaría innovadora si la iniciativa fuera sancionada por el Congreso nacional.

Lo expuesto nos permite avizorar que frente a una posible sanción del *proyecto de nuevo Código Penal* no caería caso alguno cuyo objeto procesal lo constituyan hechos previos al posible cambio legislativo, por no existir para quien resultase acusado ninguna normativa susceptible de ser aplicada con retroactividad, por resultar más benigna.

Asimismo (más allá de que la evolución de los delitos informáticos es tan dinámica como el avance de las TIC conjugado con factores de índole diversa –por ejemplo: las derivaciones propias de una inesperada pandemia como la del Covid-19–), el *proyecto de nuevo Código Penal* busca modernizar la legislación represiva, de modo tal que diversas conductas disvaliosas que al día de hoy no son delictivas, pero que entrañan riesgos o implican daños para intereses fundamentales en el marco de sociedad de la información, se vean alcanzadas por lo que es, acaso, la herramienta más poderosa de la que dispone el Estado: el derecho de ejercer el *ius puniendi*.

IV.- Anexo comparativo entre el Código Penal argentino y el *proyecto de nuevo Código Penal* en materia de delitos informáticos vigentes

Código Penal de la República Argentina	**Proyecto de nuevo Código Penal**
Artículo 128 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	**Artículo 123** 1. Se impondrá prisión de TRES (3) a SEIS (6) años, al que produjere, financiare, ofreciere, comerciare, publicare, facilitare, divulgare o distribuyere, por cualquier medio, toda representación de una persona menor de DIECIOCHO (18) años dedicado a actividades sexuales explícitas o toda

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.	representación de sus partes genitales con fines predominantemente sexuales. La misma pena se impondrá al que organizare espectáculos en vivo de representaciones sexuales explícitas en que participaren personas menores de DIECIOCHO (18) años. Si el autor actuare con fines de lucro, el mínimo de la pena de prisión se elevará a CUATRO (4) años. 2. Se impondrá prisión de CUATRO (4) meses a UN (1) año, al que a sabiendas tuviere en su poder representaciones de las descriptas en el apartado 1. Se impondrá prisión de SEIS (6) meses a DOS (2) años, al que tuviere en su poder representaciones de las descriptas en el apartado 1 con fines inequívocos de distribución o comercialización. 3. Se impondrá prisión de UN (1) mes a TRES (3) años, a la persona mayor de edad que facilitare el acceso a espectáculos pornográficos o suministrare material pornográfico a personas menores de CATORCE (14) años. **Artículo 124** Las escalas penales previstas en el artículo 123 se elevarán en un tercio en su mínimo y en su máximo: 1°) Si la víctima fuere menor de 13 años. 2°) Si el material pornográfico

	representare especial violencia física contra la víctima. 3°) Si el hecho fuere cometido por ascendiente, afín en línea recta, hermano, tutor, curador, ministro de algún culto reconocido o no, encargado de la educación o de la guarda.
Artículo 131 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.	**Artículo 122** Se impondrá prisión de SEIS (6) meses a CINCO (5) años, siempre que el hecho no importe un delito más severamente penado, a la persona mayor de edad que: 1°) Tomare contacto con una persona menor de TRECE (13) años mediante conversaciones o relatos de contenido sexual. 2°) Le requiera, por cualquier medio y de cualquier modo, a una persona menor de TRECE (13) años que realice actividades sexuales explícitas o actos con connotación sexual o le solicite imágenes de sí misma con contenido sexual. 3°) Le proponga, por cualquier medio y de cualquier modo, a una persona menor de TRECE (13) años concertar un encuentro para llevar a cabo actividades sexuales con ella, siempre que tal propuesta se acompañe de actos materiales

	encaminados al acercamiento. 4°) Realizare cualquiera de las acciones previstas en los incisos 1°, 2° y 3° con una persona mayor de TRECE (13) años y menor de DIECISÉIS (16) años, aprovechándose de su inmadurez sexual o si mediare engaño, violencia, amenaza, abuso de autoridad o de una situación de vulnerabilidad, o cualquier otro medio de intimidación o coerción. 5°) Realizare cualquiera de las acciones previstas en los incisos 1°, 2° y 3° con una persona mayor de DIECISÉIS (16) años y menor de DIECIOCHO (18) años si mediare engaño, violencia, amenaza, abuso de autoridad o de una situación de vulnerabilidad, o cualquier otro medio de intimidación o coerción.
Artículo 153 bis. 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	**Artículo 501** Se impondrá prisión de QUINCE (15) días a SEIS (6) meses, si no resultare un delito más severamente penado, al que a sabiendas accediere por cualquier medio, sin autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido. **Artículo 502** La pena será de SEIS (6) meses a DOS (2) años de prisión:

público estatal o de un proveedor de servicios públicos o de servicios financieros.	1°) Si el hecho hubiere afectado un sistema o dato informático de un organismo público estatal. 2°) Si el acceso hubiere afectado un sistema o dato informático de un proveedor de servicios públicos, de salud o financieros. 3°) Si el hecho hubiera afectado a un número indiscriminado de víctimas. Si el hecho se cometiere con el fin de obtener información sensible a la defensa nacional, el máximo de la pena de prisión se elevará a CUATRO (4) años.
Artículo 153 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	**Artículo 153** Se impondrá prisión de SEIS (6) meses a DOS (2) años y multa de DIEZ (10) a CIENTO CINCUENTA (150) días-multa, al que: 1°) Abriere o accediere indebidamente a una comunicación electrónica, una carta, un pliego cerrado, un papel privado o un despacho telegráfico, telefónico o de otra naturaleza que no le esté dirigido. 2°) Se apoderare indebidamente de una comunicación electrónica, de una carta, de un pliego, de un despacho u o de otro papel privado, aunque no esté cerrado.

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.	3°) Indebidamente suprimiere o desviare de su destino una correspondencia o una comunicación electrónica o telefónica que no le esté dirigida. 4°) Indebidamente interceptare o captare comunicaciones electrónicas o telecomunicaciones provenientes de cualquier sistema de carácter privado o de acceso restringido. Si el autor además comunicare a otro, publicare o hiciere publicar el contenido de la carta, escrito, despacho, comunicación electrónica o telecomunicación, la pena será de UNO (1) a TRES (3) años de prisión.
Artículo 157 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.	**Artículo 156** 1. Se impondrá prisión de SEIS (6) meses a DOS (2) años e inhabilitación especial, en su caso, por doble del tiempo de la condena a prisión, al que teniendo noticias por razón de su estado, oficio, empleo, profesión o arte, de un secreto cuya divulgación pueda causar daño, lo revelare sin justa causa. La misma pena se impondrá al funcionario público que revelare hechos, actuaciones, documentos o datos, que por ley debieran quedar secretos. 2. Se impondrá prisión de UNO (1) a CUATRO (4) años e inhabilitación especial de CINCO (5) a DIEZ (10) años, al funcionario o

	empleado público que ilegítimamente revelare constancias de carácter reservado o secreto relacionadas con la identificación de las personas. 3. Se impondrá prisión de CUATRO (4) a OCHO (8) años, CUARENTA Y OCHO (48) a NOVENTA Y SEIS (96) días-multa e inhabilitación absoluta perpetua, al funcionario o empleado público que indebidamente revelare la real o nueva identidad de un agente encubierto, de un agente revelador o de un informante, si no configurare una conducta más severamente penada. Si el funcionario o empleado público permitiere o diere ocasión a que otro conozca dicha información por imprudencia, negligencia o inobservancia de los reglamentos o deberes a su cargo, la pena será de UNO (1) a TRES (3) años de prisión, DOCE (12) a TREINTA Y SEIS (36) días-multa e inhabilitación especial de TRES (3) a DIEZ (10) años.
Artículo 157 bis 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;	**Artículo 157** 1. Se impondrá prisión de SEIS (6) meses a DOS (2) años, al 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

2. Ilegítimamente proporcionare o revelare a otro información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley. 3. Ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales. Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de un (1) a cuatro (4) años.	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 suprimiere, insertare o hiciere insertar datos en un archivo de datos personales. Si el autor fuere funcionario público, se impondrá, además, inhabilitación de UNO (1) a CINCO (5) años. 2. Se impondrá prisión de UNO (1) a CUATRO (4) años, al que copiare, comunicare o divulgare indebidamente el contenido de documentación o información de carácter confidencial referido en la Ley N° 26.247, si hubiere sido entregada a un inspector nacional o de la Organización o a la Autoridad Nacional, directamente o por intermedio de un Estado extranjero.
Artículo 173 Sin perjuicio de la disposición general del artículo precedente, se considerarán casos especiales de defraudación y sufrirán la pena que él establece (prisión de un mes a seis años): 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	**Artículo 173** Sin perjuicio de la disposición general del artículo 172, se considerarán casos especiales de defraudación y se impondrá la misma pena que establece aquel artículo (prisión de un mes a seis años): 15) Al que defraudare mediante el uso de una tarjeta de compra, crédito o débito, que hubiese sido

del legítimo emisor mediante ardid o engaño, o mediante el uso no autorizado de sus datos, aunque lo hiciere por medio de una operación automática. 16.	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.
Artículo 173 Sin perjuicio de la disposición general del artículo precedente, se considerarán casos especiales de defraudación y sufrirán la pena que él establece (prisión de un mes a seis años): 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.	**Artículo 500** Se impondrá prisión de UN (1) mes a SEIS (6) años, al que defraudare a otro mediante la introducción, alteración, borrado o supresión de datos de un sistema informático, o utilizando cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos.
Artículo 183 Será reprimido con prisión de quince días a un año, el que destruyere, inutilizare, hiciere desaparecer o de cualquier modo dañare una cosa mueble o inmueble o un animal, total o parcialmente ajeno, siempre que el hecho no constituya otro delito más severamente penado. En la misma pena incurrirá el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o	**Artículo 494** Se impondrá prisión de QUINCE (15) días a UN (1) año o UNO (1) a DOCE (12) días-multa, al que ilegítimamente y sin autorización de su titular alterare, destruyere o inutilizare datos, documentos, programas, sistemas informáticos o registros informáticos de cualquier índole. Si los datos, documentos o programas afectados fueren aquellos protegidos por la Ley N° 24.766, la escala penal prevista se elevará en un tercio del mínimo y del máximo.

introdujere en un sistema informático, cualquier programa destinado a causar daños.

Artículo 184

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

1. Ejecutar el hecho con el fin de impedir el libre ejercicio de la autoridad o en venganza de sus determinaciones;

2. Producir infección o contagio en aves u otros animales domésticos;

3. Emplear substancias venenosas o corrosivas;

4. Cometer el delito en despoblado y en banda;

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

Artículo 495

La pena será de prisión de TRES (3) meses a CUATRO (4) años:

1°) Si el hecho se ejecutare en documentos, programas o sistemas informáticos públicos.

2°) Si el hecho se cometiere 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.

3°) Si el daño recayere sobre un bien perteneciente al patrimonio cultural de la NACIÓN ARGENTINA o de un Estado extranjero.

Artículo 496

La pena será de prisión de UNO (1) a CINCO (5) años si, por el modo de comisión:

1°) El hecho hubiere afectado a un número indiscriminado de sistemas informáticos.

2°) El hecho hubiere afectado el funcionamiento de servicios públicos esenciales o la provisión de bienes de primera necesidad.

3°) El hecho hubiere creado una situación de peligro grave para la

transporte u otro servicio público.	sociedad. **Artículo 497** Se impondrá prisión de UNO (1) a CINCO (5) años, al que ilegítimamente y sin autorización de su titular, mediante cualquier artificio tecnológico, mecanismo de cifrado o programas maliciosos, obstaculizare o interrumpiere el funcionamiento de un sistema informático ajeno o impida a los legítimos usuarios el acceso a los datos del sistema, siempre que el hecho no importe un delito más severamente penado. **Artículo 498** Se impondrá prisión de QUINCE (15) días a UN (1) año o UNO (1) a DOCE (12) días-multa, al que vendiere, distribuyere, hiciere circular o introdujere en un sistema informático cualquier programa destinado a causar daños.
Artículo 197 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.	**Artículo 192** Se impondrá de SEIS (6) meses a TRES (3) años de prisión, si el hecho no constituyere un delito más severamente penado: 1°) Al que, aun sin crear un peligro común, empleare cualquier medio para detener o entorpecer la marcha de un medio de transporte público.

	2°) Al que, sin autorización, aun sin crear un peligro común, empleare cualquier medio para detener o entorpecer la marcha de un medio de transporte privado. 3°) Al que, aun sin crear un peligro común, ejecutare cualquier acto tendiente a interrumpir o entorpecer el funcionamiento de los servicios públicos de comunicación telefónica, radiofónica, satelital o electrónica, de provisión de agua, de electricidad o de sustancias energéticas o resistiere con violencia su restablecimiento
Artículo 255 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 ($	**Artículo 255** Se impondrá prisión de SEIS (6) meses a CUATRO (4) años, al 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, se impondrá, además, inhabilitación especial por el doble del tiempo de la condena a prisión. Si el hecho se cometiere por imprudencia o negligencia, impericia en su arte o profesión, o inobservancia de los reglamentos o deberes a cargo

12.500).	del depositario, a éste se le aplicará de DOS (2) a DOCE (12) días-multa.