ISSN 2250-7558

Derecho Penal

AÑO III NÚMERO 7

Delitos Informáticos

Directores: Alejandro Alagia - Javier De Luca - Alejandro Slokar

Ministerio de Justicia y Derechos Humanos
Presidencia de la Nación

Infojus
SISTEMA ARGENTINO DE INFORMACIÓN JURÍDICA

AÑO III - NÚMERO 7

Derecho Penal

ISSN 2250-7558
Revista Derecho Penal
Año III - N° 7 - Mayo 2014
Editorial Ministerio de Justicia y Derechos Humanos de la Nación, Sarmiento 329, C.P. 1041AFF, C.A.B.A.
Editado por la Dirección Nacional del Sistema Argentino de Información Jurídica.
Directora: María Paula Pontoriero
Directores Editoriales: Alejandro Alagia - Javier De Luca - Alejandro Slokar
Correo electrónico: ediciones@infojus.gov.ar

Francisco Figueroa - Antonela C. Ghezzi
María Ángeles Ramos - Emiliano Espejo

Colaboradores

Diego García Yomha - Juan Pablo Iriarte
Santiago Martínez - Nahuel Martín Perlinger

Colaboradores
Sección Organización Judicial

Consejo Académico

Editorial

En los tiempos que corren, desde hace no más de treinta años, tanto individuos como organizaciones con acceso a la tecnología de las comunicaciones comparten información a lo largo y ancho del planeta. Los intercambios electrónicos dieron un nuevo impulso, de manera exponencial, a todo tipo de comunicaciones oficiales y privadas, acercaron a las personas y ampliaron la distribución de la información de una manera inimaginable, expandiendo la globalización social y económica a límites nunca antes conocidos, a la vez que se convirtió en un poderoso medio de organización y manifestación de opiniones y acciones tanto de denuncia como de apoyo a los distintos gobiernos.

Pero, paralelamente, ese proceso trajo consigo todo tipo de actividades dañinas a los derechos de las personas involucradas en los procesos de intercambio de información, algunas de ellas consistentes en nuevas formas de realización de viejos delitos, y otras cuya criminalización tuvo que ser seriamente considerada. Así, aparecieron los diversos tipos de hacking (una vulgar traducción sería la de expertos que acceden o manipulan o atacan archivos y redes de comunicación electrónica) la distribución de pornografía infantil, acosos sexuales y hostigamientos de todo tipo, difusión de propagandas de odio y discriminación, grandes fraudes o daños de proporciones contra enemigos comerciales o políticos, el espionaje privado u oficial, violaciones de secretos oficiales y privados con fines extorsivos, delitos de la propiedad intelectual, todo tipo de injerencias en la privacidad de las personas, y conflictos con las distintas modalidades de la libertad de expresión, entre otros.

Además, estas nuevas actividades crearon serios problemas jurisdiccionales, tanto para el principio de doble incriminación como para su investigación, la cooperación internacional y su juzgamiento, porque las acciones se realizan en distintos países, con impacto infinito.

La experiencia de estos años demostró que no era válido el inicial criterio que propiciaba la regulación y criminalización porque las principales víctimas eran las democracias jóvenes, emergentes, de incipiente desarrollo tecnológico. Hoy se sabe que eso puede ser así, pero también, que los peores ataques a los sistemas de comunicación electrónicos, oficiales y priva-

dos, son parte de determinadas políticas de gobierno de países poderosos, que lo hacen entre ellos también, y que es imposible alcanzar las nuevas formas que conforman los ataques con la regulación y la criminalización. La tecnología siempre va adelante en una carrera desigual, aunque la sociedad de que se trate tenga la tecnología más avanzada.

Las prácticas que en tan poco tiempo ya han pasado a ser clásicas son, por ejemplo, las de observación de los patrones de tráfico de datos para sacar conclusiones sobre los usuarios de las redes; el husmear en la información guardada en los archivos; la modificación de archivos y de claves; el falseamiento y suplantación de identidades y claves para engañar y extraer información; la inserción de virus en los sistema para la destrucción de archivos o para observar todos los movimientos; y la búsqueda dentro de los sistemas para alojar en sus huecos determinados detectores y recolectores de la información que interesa. Los términos de las distintas conductas y prácticas generalmente están en inglés, y se han multiplicado con los años. Se trata de un nuevo lenguaje, donde pocas palabras describen conductas o procesos complejos. Y la creatividad en ese sentido, no parece tener un techo a la vista.

En este número de nuestra revista se tratan muchas de estas cuestiones. También se incluye un profundo cuestionario, dividido en cuatro partes (Derecho penal parte general, penal parte especial, procesal penal y penal internacional) formulado por la Asociación Internacional de Derecho Penal (AIDP) al grupo argentino, debido a que este año 2014 se celebrará el tradicional congreso internacional, precisamente, sobre delitos informáticos. De ese cuestionario y sus respuestas, se desprenden los problemas involucrados. Asimismo, como ya es corriente, se incluyen otros trabajos. Por su importancia para los derechos humanos de las personas sometidas a encierro y en particular a las que padecen en esa situación graves enfermedades mentales, ponemos para conocimiento del público el importante trabajo de investigación, asistencia y contención que realiza la Defensoría General de la Ciudad Autónoma de Buenos Aires con los presos de esta jurisdicción. Y también acercamos un importante estudio sobre organización judicial, especialmente referido a las audiencias orales.

Buenos Aires, otoño de 2014.

Los directores

Índice General

Doctrina p. 1

Doctrina

El delito de contacto telemático con menores de edad con fines sexuales

Análisis del Código Penal argentino y del *Estatuto da Criança e do Adolescente* brasileño

por **GUSTAVO EDUARDO ABOSO**[1]

1 | Introducción

1.1 | El nuevo art. 131 del Código Penal argentino

La ley 26.904[2] introdujo el nuevo art. 131 al Código Penal que reza de la siguiente forma:

> "Será reprimido 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".

(1) Abogado (UBA). Master en Derecho por la Universidad de Palermo. Profesor de la Universidad Nacional de Buenos Aires (UBA) y del curso de Posgrado de Derecho Penal de la Universidad de Belgrano. Defensor Oficial en el Poder Judicial de la Ciudad Autónoma de Buenos Aires.

(2) BO 11/12/2013.

El desarrollo tecnológico de los medios de comunicación trajo consigo un efecto negativo que lamentablemente se cristaliza en la irrupción de nuevas formas de comportamientos que atentan contra la integridad sexual de los menores de edad. En este caso, la reciente introducción del art. 131 al Código Penal confirma esta tendencia que se ha experimentado en otros ordenamientos penales.(3)

Así pues, como afirma Sieber, el peligro que encierra el uso abusivo de los ordenadores se fundamenta en puntos de vista cuantitativos y cualitativos: la lesividad de la moderna sociedad informática, que no se restringe al uso personal de los computadores y los sistemas informáticos, sino que atentan contra la paulatina dependencia de la sociedad moderna de la operatividad de los sistemas informáticos. Por mencionar algunos ejemplos, la mayoría de las transacciones económicas y financieras se encarrilan mediante el uso de los sistemas computarizados; la producción de las fábricas depende cada día más de la intervención de procesos automatizados e informatizados; los sistemas de drenajes y de distribución de aguas dependen también de dichos sistemas y procesos; etcétera.(4)

Por lo general, desde la experiencia recogida en nuestro país y a nivel mundial, se ha impuesto la necesidad de ampliar la barrera de punición a conductas que son propicias para la consumación de atentados contra la indemnidad sexual de los menores de edad. La facilidad y disponibilidad que tienen hoy en día los menores de edad de acceder a los sistemas telemáticos y así ampliar de manera exponencial el horizonte de su comunicación social ha determinado cambios de conductas y estrategias de los ciberacosadores y de grupos de pedófilos que se aprovechan de la candidez de sus víctimas y que, bajo la apariencia de un falso perfil de usuario, contactan a menores de edad con el fin de menoscabar su integridad sexual. En este contexto, los que pretenden atentar contra la indemnidad sexual de los menores de edad aprovechan precisamente los foros, blogs, *chat-rooms* o demás formas de comunicación para buscar, individualizar

(3) Por ejemplo, el art. 183 ***bis*** del Cód. Penal español; art. 227-22-1 del Código Penal francés; art. 609-undecies del Código Penal italiano; s. 15 *Sexual Offences Act*, 2003 [SOA] del Reino Unido; art. 1 *Protection of children and prevention of sexual Offences*, Act. 2005, de Escocia; art. 172.1 *Criminal Code* de Canadá, §§ 2422 y 2425 del United States Code, entre otros.

(4) Sieber, Ulrich, *Multimediarecht, Strafrecht und Strafproze*ß*recht*, [en línea] http://www.jura.uni-muenchen.de/sieber/article, p. 25.

e identificar a sus víctimas. En la "Exposición de Motivos" de esta nueva reforma se describe este fenómeno mundial y la necesidad de adecuar la legislación local a los estándares internacionales fijados por los tratados en esta materia.

En este cuadro debe mencionarse la **Decisión marco 2004/68/JAI del Consejo de la Unión Europea, del 22 de diciembre de 2003, relativa a la Lucha contra la Explotación Sexual de los Niños y la Pornografía Infantil, y a**l Convenio sobre la Protección de Niños contra la Explotación Sexual y el Abuso Sexual, del 25 de octubre de 2007, que estableció los parámetros normativos de la regulación de esta figura en el ámbito de la Eurozona (art. 23).[5]

Es frecuente observar en la doctrina y la jurisprudencia, incluso en el diálogo académico, la aplicación errada, distorsionada, que se hace de la categoría "delitos informáticos" para englobar de esta forma aquellos comportamientos caracterizados por el empleo abusivo de una terminal que provoca perjuicios económicos a terceros, o bien permite el ingreso ilegítimo a una base de datos, o directamente la introducción de un virus en el sistema telemático.[6] Quizás sea más práctico para el uso del

(5) Council of Europe, Treaty Series 201, "Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse", Lanzarote, 25/10/2007, [en línea] http://www.google.com.ar/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CCgQFjAA&url=http%3A%2F%2Fconventions.coe.int%2FTreaty%2FEN%2FTreaties%2FWord%2F201.doc&ei=ueVDU8unEeG3sASIo4CYDQ&usg=AFQjCNF3cXV9VNsuo4qmOy1IZIdDDugu0g&bvm=bv.64367178,d.cWc

(6) Véase, Arocena, Gustavo, "De los delitos informáticos", en *Revista de la Facultad de Derecho, Universidad Nacional de Córdoba*, vol. 5, nº 1, 1997, p. 44 y ss., donde reproduce de forma sintética la diversidad de opiniones existentes en la doctrina argentina sobre el contenido y alcance del término "delitos informáticos". Según este autor, la conceptualización del delito informático debería abarcar tanto las modalidades criminales que utilizan un sistema informático como vehículo para la perpetración de distintos ilícitos, como cuando dicho sistema informático se transforma en el objeto del comportamiento delictivo. En igual sentido, Carrera de Hairabedián, Marcela, "Algunas consideraciones sobre los delitos informáticos", *Foro de Córdoba*, nº 63, p. 57 y ss. Resulta conveniente mencionar que si bien es correcta la afirmación de que los denominados "delitos informáticos" afectan la propiedad y la intimidad de las personas, una acepción amplia de la criminalidad informática impide descubrir una nueva realidad social que impone al derecho penal modificar y adecuar su arsenal represivo de cara a los nuevos desarrollos tecnológicos alcanzados por la humanidad, por un lado; mientras que, por otro, dicho tipismo rehúye al reconocimiento de una **necesidad funcional** de las sociedades contemporáneas que se organizan paulatinamente, sumado a otras contingencias, sobre el almacenamiento, procesamiento, circulación y valor de la información. La tesis propuesta en este trabajo pretende reconocer la autonomía funcional de los delitos informáticos frente a otras modalidades criminosas que atentan en igual medida contra la intimidad y la propiedad de terceros. De ahí que aquellas acciones que consistan en el ingreso

lenguaje cotidiano referirse indistintamente a uno u otro suceso delictivo relacionado con el uso de una terminal, pero dicho empleo laxo genera en el otro una ambigüedad que contribuye a fraguar una realidad distinta que impide, en una primera reflexión, indagar sobre cuál debería ser el verdadero interés tutelado que se esconde detrás de esta especie de infracciones. Permítaseme describirlo de la siguiente forma: existe consenso para calificar de estafa informática a la utilización de una terminal para perfeccionar una maniobra fraudulenta.(7)

ilegítimo a una base de datos, la utilización no autorizada de un ordenador, la destrucción de un sistema informático, el borrado de la información almacenada mediante el empleo de un virus o la interrupción temporal de dicho servicio, entre otras, son manifestaciones ofensivas que si bien podrían asociarse en algunos casos a figuras delictivas actualmente reguladas, dicha equiparación no traspasaría el umbral de una relación simétrica comisiva, mas no sería suficiente para reconocer la funcionalidad propia de la información, en su doble acepción de objeto y acción. Al respecto, Aboso, Gustavo y Zapata, María Florencia, *Cibercriminalidad y derecho penal*, BdeF, Buenos Aires-Montevideo, 2006, p. 15 y ss.

(7) Guibourg, Ricardo; Allende, Jorge y Campanella, Elena *Manual de informática jurídica*, Bs. As., Astrea, 1996, § 86, p. 273, afirman que el delito informático no constituye una nueva categoría delictiva. Esta aseveración es correcta siempre y cuando el intérprete se sitúe en la dimensión **instrumental** del uso abusivo de un ordenador. Es cierto que los fraudes cometidos mediante Internet, por ejemplo, no modifican en nada la esencia de la defraudación y sólo el **medio empleado** revela, en todo caso, la fase de modernidad de nuestras sociedades, en las que el uso tecnológico resulta adaptado por el hombre para la consecución de sus fines, lícitos o ilícitos, buenos o malos, pero siempre radica en la propia naturaleza del hombre dicha asignación de medios. En cambio, esta perspectiva puede ceder frente a otra mucho más específica: la de considerar a la **información en sí** —**al flujo de esa información mediante los canales informáticos**—, como un interés digno de tutela especial que adquiere una entidad propia despojada de toda pretensión utilitarista. En este artículo se intentará desentrañar esta nueva dimensión de la **información** como sujeto de tutela penal, sin olvidar que la información en su dimensión **funcional** inauguró un permanente proceso expansivo que trasciende en muchos aspectos la acotada imagen de la intimidad individual, cuyo papel adquiere en la actualidad una preeminencia significativa en el funcionamiento y desarrollo de los mercados mundiales. Esta valorización de la información, vinculada al avance incesante de la tecnología y sus derivados, provocan el derrumbe de muchas fronteras hasta hace poco tiempo infranqueables. Piénsese, por ejemplo, en el método de desciframiento del genoma humano y la factibilidad de desentrañar los orígenes del ser humano, incluso la posibilidad de alterar su subjetividad. Este nuevo portal de conocimientos y posibilidades abierto por las ciencias coloca al hombre en una disyuntiva moral y ética que trastoca su propia existencia: la de jugar a ser Dios. Así, entonces, el diagnóstico genético permite prever enfermedades o predisposiciones congénitas de la persona y esta información genética adquiere así una importancia en una sociedad caracterizada por la alta competitividad (por ejemplo, en la selección de empleados o dirigentes de una empresa) y la exuberante pleitesía a las leyes del mercado de capitales (por ejemplo, la evaluación de riesgos para las empresas aseguradoras frente al cliente con predisposiciones a las enfermedades cardíacas comprobadas mediante métodos genéticos). Sobre esta problemática en particular, Habermas, Jürgen, *El futuro de la naturaleza humana*, (trad. por R. S. Carbó), Barcelona, Paidós, 2002. Al respecto, Aboso y Zapata, *Cibercriminalidad y derecho penal, op. cit*, pp. 15 y ss./29 y ss.

En este campo se distingue entre la "criminalidad de la red" (*Netzkriminalität*) que se concentra en el uso abusivo de los ordenadores en la red informática pública, y la llamada "criminalidad multimedia" (*Multimedia-Kriminalität*) que se proyecta en el mercado competitivo de los diversos multimedios y la convergencia de los aparatos digitalizados, como la computadora personal, los aparatos radiales o los de telecomunicaciones, que posibilitará que en el futuro cercano la difusión de la información y la trasmisión de la comunicación amplíen sus fronteras (la llamada era digital).(8)

2 | El delito de contacto telemático con menores de edad con fines sexuales

2.1 | Análisis dogmático

Volviendo al comentario del art. 131 CP, el bien jurídico tutelado es el normal desarrollo psico-biológico sexual de los menores de dieciocho años.(9) En este ámbito, las agresiones sexuales contra menores de edad suelen clasificarse según la existencia o no de contacto sexual ilícito. Esta modalidad de acoso telemático se caracteriza por la falta de contacto sexual,

(8) Sieber, Ulrich, *Multimediarecht, Strafrecht und Strafprozeβrecht*, cit., p. 23.

(9) Schweizer, Katinka, "Grundlagen der psychosexuellen Entwicklung und 'ihrer Storungen'", *Sexuelle Identität und gesellschaftliche Norm*, Gunnar Duttge, Wolfgang Engel und Barbara Zoll (Hg.), Göttinger Schriften zum Medizinrecht, Bd. 10, Universitätsverlag Göttingen, 2010, p. 11 y ss. La sexualidad se vincula en nuestros días con aspectos biológicos, psicológicos y sociales que definen la personalidad sexual del individuo. La autora analiza la teoría de Freud sobre el desarrollo psíco-sexual y las diversas fases que incluye dicho desarrollo (oral, anal, genital y latencia) hasta desembocar en la pubertad. Esta división ha sido ampliada en la actualidad con los nuevos estudios sobre la sexualidad humana, en general, existe consenso en agrega una fase intermedia identificada con la fantasía infantil omnipotente que se relaciona con la fantasía de la bisexualidad en los menores entre los dos y cuatro años. Sobre el bien jurídico tutelado en la doctrina española, Silva Sánchez, Jesús-María (dir.), *Lecciones de Derecho Penal. Parte especial*, Barcelona, Atelier, 2006, pp. 107/108; Zugaldía Espinar y Marín de Espinosa Ceballos (dirs.), *Derecho penal. Parte especial*, t. I, Valencia, Tirant lo Blanch, 2011, p. 286 y ss.; Rubio Lara, Pedro, "Acoso sexual de menores por Internet: Cuestiones penales, procesales penales y civiles", en AA.VV., *Ciberacoso: la tutela penal de la intimidad, la integridad y la libertad sexual en internet*, Valencia, Tirant lo Blanch, 2010, p. 145 y ss. Al respecto, Aboso, Gustavo, *Código Penal de la República Argentina comentado, concordado y con jurisprudencia*, BdeF, Buenos Aires-Montevideo, 2012, p. 575 y ss.

pero se demuestra como una conducta de facilitación, ya que el autor debe perseguir el propósito de un ulterior contacto sexual.

El uso de la coacción estatal ha sufrido en los últimos tiempos —en el marco de la criminalidad informática en general y respecto de los delitos sexuales relacionados con la pornografía infantil en especial—, un auge sorprendente. Si bien es cierto que los tratados internacionales en esta materia —las Convenciones de Budapest y Lanzarote—, han procurado armonizar la legislación penal en el ámbito europeo, con una fuerte influencia más allá de sus fronteras, puede percibirse sin mayores esfuerzos que los medios de intervención utilizados por el derecho penal no siempre respetan el principio de lesividad, o al menos, resulta forzada la relación de la conducta prohibida y el fundamento material de dicha prohibición en relación con el principio de la protección de bienes jurídicos.(10)

A modo de ejemplo, la regulación del delito de distribución y posesión de material pornográfico adoptada por el § 184c del Código Penal alemán. En este caso, han surgido divergencias normativas a nivel nacional y europeo sobre el alcance del término "niño". Específicamente, el instrumento internacional europeo habla de un menor de dieciocho años, mientras que la legislación penal alemana lo refiere para los menores de catorce años (§176 1 StGB), y la ley penal juvenil establece su alcance a los menores de dieciocho años (§ 1, Abs. 2, JGG). Sobre la represión del consumo de pornografía infantil, al castigarse en muchos ordenamientos penales la simple tenencia, o bien, como sucede en el nuestro, cuando dicha tenencia tenga una finalidad de comercialización o distribución, han despertado las críticas de la doctrina sobre el fundamento material de dicha coacción estatal desde el punto de vista del principio de lesividad.(11)

Desde esta perspectiva, la nueva regulación del delito de *grooming* aparece signada por este déficit, ya que si bien el motivo de esta nueva forma

(10) Sobre la crítica a la teoría del bien jurídico, Neumann, Ulfrid, "Alternativas: Ninguna. Sobre la crítica más reciente a la teoría personal del bien jurídico", (trad. Carmen Eloisa Ruiz), *Cuadernos de Política Criminal*, nº 93, 2007, p. 5 y ss.

(11)Heinrich, Manfred, *"Strafrecht als Rechtsgüterschutz ein Auslafmodell? Zur Unverbrüchlichkeit des Rechtsgutsdogmas"*, en *Festschrift für Claus Roxin zum 80*, Manfred Heinrich, Christian Jäger et al. (Hrsg.), Bd. 1, De Gruyter, Berlin, 2011, pp. 131 y ss. / 135 y ss. Sobre la reforma de los delitos sexuales en España, Cancio Meliá, Manuel, "Una nueva reforma de los delitos sexuales contra la libertad", en *La Ley Penal*, nº 80, año VIII, marzo 2011, pp. 5 y ss. / 15 y ss.

de criminalización del uso abusivo de los medios informáticos tiende a la tutela de los menores de edad, lo cierto es que el medio utilizado y la técnica legislativa carecen en todo caso de un estilo refinado e idóneo para cumplir con tal propósito sin necesidad de sacrificar al principio de lesividad en el altar de la creciente expansión del derecho penal. Como veremos a continuación, esta conducta de contactar mediante medios telemáticos a menores de edad con un propósito sexual ha sido criticada de manera uniforme en todos los países. La principal objeción que se le formula consiste en su excesiva ambigüedad y el inocultable adelantamiento de la barrera de punición[12] que representa la mera punición de un contacto telemático con un menor de dieciocho años sin recurrir al expediente del engaño o la seducción.

La determinación de la condición etaria del sujeto pasivo agrega un mayor grado de confusión a los parámetros normativos utilizados por el legislador. En especial, debemos recordar aquí que a partir de los trece años el titular del bien jurídico puede mantener contactos sexuales con terceros. En este sentido, a partir de los catorce años puede serle suministrado material pornográfico o facilitársele el acceso a un espectáculo pornográfico (art. 128), mientras que por debajo de los dieciocho años se castigan las exhibiciones obscenas (art. 129). Ni hablar de las edades mínimas fijadas para la tolerancia de los contactos sexuales con acceso carnal. En síntesis, la disparidad punitiva que puede observarse entre las figuras que tutelan la indemnidad sexual de los menores de edad adolece de una peculiar esquizofrenia normativa que se refleja en la falta de armonía en las edades mínimas requeridas para considerar punible una conducta, sin atender al parámetro objetivo de la existencia o no de contacto sexual con los menores de edad. De esta manera, se castiga con una pena que orilla los cuatro años el simple acercamiento telemático con un menor de edad, pero si se comete un abuso sexual simple, la amenaza de pena es idéntica. Así y todo, si se le entrega material pornográfico o se le allana el camino para acceder a un espectáculo de esa naturaleza a un menor de catorce años, la expectativa de pena no superará los tres años. En cambio, si el autor se

(12) Muñoz Conde, Francisco, *Derecho penal. Parte especial*, Valencia, Tirant lo Blanch, 2013, p. 230; Salvadori, Ivan, "Posseso di pornografía infantile, acceso a siti pedopornografici, child-grooming e tecniche di anticipazione della tutela penale", p. 20 y ss.; Riquert, Marcelo, "Ciberacoso sexual infantil ('*cibergrooming*')", [en línea] http://www.pensamientopenal.com.ar/sites/default/files/cpc/art._131_ciber_acoso_sexual_infantil_grooming.pdf; Aboso, Gustavo, *Código Penal..., op. cit.*, art. 131.

exhibe desnudo ante el menor de trece años, la pena aplicable en su máxima expresión será de cuatro años de prisión, mientras que si el sujeto pasivo de este delito de exhibiciones es un menor de dieciocho años que no consiente dicho acto, la expectativa de pena será de idéntica gravedad.

El llamado "ciberacoso",[13] o directamente *child grooming*, se caracteriza por:

a. La falta de contacto personal con el sujeto pasivo;

b. La particularidad del medio utilizado (medio telemático) y;

c. La finalidad que persigue el autor (sexual).

a. La falta de contacto personal con el sujeto pasivo

En los delitos sexuales, la distinción entre contacto corporal o no con la víctima determina la mayor o menor gravedad del comportamiento reprimido.[14] Este baremo objetivo de valoración de la gravedad de lo injusto de una conducta dolosa en este campo del derecho penal sexual no ha sido observado, conforme se detalló precedentemente, en función de la gravedad de la pena prevista en relación con otros comportamientos ilícitos de naturaleza sexual donde sí está presente el contacto físico entre el autor y la víctima. Este delito de *child grooming* se erige sobre la base de la ausencia de todo contacto corporal entre el autor y la víctima.

b. La particularidad del medio utilizado

El flamante art. 131 tiene un ámbito de aplicación acotado a los medios telemáticos en general. Este tipo de conductas abusivas se manifiestan con especial virulencia en el uso de los medios de comunicación electrónicos. Así, la posibilidad de entablar una comunicación en tiempo real con otra persona o bien mediante el uso de correos, mensajes o cualquier tipo de transferencia de datos electrónicos permite que los menores de edad se encuentren expuestos de manera directa a este tipo de contactos con fi-

(13) Hay objeciones sobre el uso de este término basadas en que esta figura no se trata propiamente de un acoso, ya que ella presupone una relación de dependencia. Sobre el contenido y alcance de este término, véase Pardo Albiach, Juan, "Ciberacoso: Cyberbullying, grooming, redes sociales y otros peligros", en *Ciberacoso: la tutela penal..., op. cit.*, p. 54 y ss.

(14) Dessecker, Axel, "Veränderungen im Sexualstrafrecht. Eine vorläufige Bewertung aktueller Reformbemühungen", *Neue Zeitschrift für Strafrecht*, Heft 1/1998, p. 1 y ss.; Etzioni, Amitai, *Los límites de la privacidad*, (trad. Alexander López Lobo), BdeF, Bs. As.-Montevideo, 2012, p. 72.

nes sexuales.[15] Nuestra norma establece como medio apto para cometer este delito a los telemáticos, pero en esta esta delimitación ha sido criticada, en especial, porque también el uso de otros medios de comunicación (por ejemplo, cartas o anuncios) ofrecen un punto propicio para la acción de los acosadores. La restricción típica al medio telemático prevista por la norma en comentario no debe hacernos pensar que este fenómeno se localiza de manera unilateral en el uso de estos medios, ya que también debería contemplarse la posibilidad de los contactos personales donde el autor ejerce también una influencia sobre los menores de edad.[16] De hecho, las legislaciones como la escocesa y la inglesa no aluden al medio informático para reprimir dicha conducta de *child grooming*.

Sobre los medios telemáticos para la comisión de este delito, la jurisprudencia anglosajona ha considerado que el envío de mensajes de texto a una menor de trece años que padecía defectos psíquicos para mantener relaciones sexuales era una conducta punible a la luz de la *Sexual Offences Act*.[17] También el contactarse con menores de dieciséis años a través de la *website* con un propósito sexual.[18] Tampoco se exige que la finalidad sexual que motiva el accionar del autor haya sido satisfecha de manera inmediata,[19] ya que el contacto indebido con el menor de edad se presenta en realidad como la antesala para la comisión de una agresión sexual.

La acción típica consiste en contactar a un menor de dieciocho años con el propósito de que el sujeto pasivo realizare actos de naturaleza sexual. Se trata de un delito de peligro. La conducta del autor debe consistir en mantener contactos mediante medios o dispositivos electrónicos de comunicación con un menor de edad. El contacto por sí solo aparece como un acto preparatorio para la comisión de otro delito de naturaleza sexual, cuya represión se ha visto confirmada por la multiplicidad de casos que se

(15) Marco Marco, Joaquín, "Menores, ciberacoso y derecho de la personalidad", en AA.VV, *Ciberacoso: la tutela penal..., op. cit.*, p. 98 y ss.

(16) Díaz Cortés, Lina,"El denominado *child grooming* del art. 183 ***bis*** del Código Penal: una aproximación a su estudio", Madrid, *Boletín del Ministerio de Justicia de España*, año LXVI, n° 2138, 2012, p. 6.

(17) *R. v. Mohammed* [2006] EWCA Crim. 1107; *R. v. Harrison* [2008] EWCA Crim 3170.

(18) *R. v. Wilson* [2006] EWCA Crim. 505.

(19) *R. v. Abdullahi* [2007] 1 WLR 225.

presentan diariamente sobre el abuso sexual de menores de edad.[20] Ciertamente no ha sido afortunado el modo de tipificar esta conducta, ya que por lo general esta figura de *child grooming* apunta de manera basal a evitar el contacto fraudulento con el menor de edad. Tal como está regulado el actual art. 131, ese contacto con un menor de edad sólo será punible cuando el autor tuviese en miras cometer un delito contra la integridad sexual. De más está decir lo ambiguo de la materia de prohibición, puesto que los menores de edad de trece años en adelante pueden mantener contactos sexuales con terceros, en consecuencia, si una persona de dieciocho años mantiene contacto telemático con un menor de diecisiete con el propósito de mantener algún tipo de relación sexual, estaría expuesto a la comisión de este delito. La falta de certeza de la acción prohibida, y los contornos difusos utilizados para la represión de esta conducta, seguramente provocarán una aplicación desmedida de esta figura. Por lo demás, si existiese un conocimiento previo de las partes involucradas —por ejemplo, dos alumnos de un establecimiento educativo—, uno de dieciocho años y el otro de diecisiete años, y los contactos realizados por medio de Internet tuviesen un contenido sexual, por ejemplo, que la menor de edad le envíe una foto de su cuerpo desnudo, o aquél la incitase a realizar conductas autorreferentes sobre su cuerpo con la intención de satisfacer sus deseos sexuales, en todos estos casos dicho contacto podría ser objeto de una investigación penal como consecuencia de la denuncia formulada por los progenitores y pese a la anuencia de la presunta víctima.

La determinación de la edad de la víctima en la franja de los menores de dieciocho años contemplada por la figura significa un excesivo y arbitrario adelantamiento de la barrera de punición de estas conductas caracterizadas por la falta de contacto físico entre el autor y la víctima. Por lo demás, se muestra como una expresión de paternalismo desmedido al no tener en cuenta el consentimiento de los menores de edad, lo cual trastoca el principio de progresividad de la tutela penal dispensada a los menores de dieciocho años. Ese adulto de dieciocho años puede mantener relaciones sexuales con una persona a partir de los trece años de edad, pero si se contacta por medio de las redes telemáticas y le ofrece mantener las mis-

(20) En uno de los primeros casos de *child grooming* sentenciados en los Estados Unidos, el autor, una persona de 37 años de edad, se contactó con menores de edad para inducirlos en la participación de actividades sexuales ilegales, sumado a la posesión y distribución de material pornográfico infantil (US Court of Appeals Eleventh Circuit, "*United States of America vs. J. A. Penton*", 25/5/2010).

mas relaciones sexuales, estaría expuesto a una eventual denuncia penal y podría ser responsabilizado penalmente por la comisión de este delito.

Por este motivo, en la legislación española, el actual art. 183 *bis* reprime el contacto de menores de trece años a través de Internet, teléfono o de cualquier otra tecnología de la información y la comunicación. La doctrina española ha criticado esta figura por representar la punición de un acto preparatorio y así un adelantamiento de la barrera de punición.(21) Por su parte, el art. 15 de la *Sexual Offences Act*, reprime la conducta de tener contacto o comunicarse con un menor de dieciséis años, mientras que el art. 227-22-1 de Código Penal francés sólo requiere que se trate de un menor de quince años o una persona que se presentase como tal.

Justamente, la finalidad político-criminal de punir esta conducta ha sido la de evitar cualquier tipo de contacto fraudulento con los menores de edad. El art. 131 CP ha prescindido de esta modalidad fraudulenta para abocarse a reprimir lisa y llanamente cualquier contacto a través de ese medio con un menor de dieciocho años, cuyo propósito ulterior sea de naturaleza sexual. En este punto hubiese sido más apropiado exigir que un contacto fraudulento con un menor de edad (que puede contabilizarse de manera objetiva mediante el uso de cuentas de correo electrónicas falsas, el uso de nombres falsos a los efectos de ocultar la edad, el género o el empleo de herramientas informáticas idóneas para evitar el rastreo o la ubicación del usuario), ya que dicha modalidad es la que ha caracterizado en realidad los casos de contactos abusivos por ese medio. Haciendo un paralelismo con el delito de estupro, dicho contacto telemático debería reunir las notas de una relación de preeminencia entre el autor y su víctima.

Este fenómeno de la cibercriminalidad adquiere relevancia cuando los adultos emplean de modo engañoso un perfil de usuario de un menor de edad, con sus usos y costumbres (modo de escritura, expresiones, modismos, etc.) que sean idóneos para determinar el error del menor de edad sobre la identidad, edad o género del usuario y sus ulteriores intenciones.

En cuanto a la modalidad utilizada, el art. 131 CP no demanda una modalidad comisiva determinada, salvo la del medio telemático del contacto,

(21) Muñoz Conde, Francisco, *Derecho penal. Parte especial*, Valencia, Tirant lo Blanch, 2012, p. 230.

pero hubiera sido mejor la demanda de una asunción de identidad falsa, es decir, la de proporcionar datos personales al sujeto pasivo que no se condicen con los verdaderos. Esto bien puede suceder mediante la consignación o el almacenamiento de datos personales falsos, especialmente el nombre, el apellido y la edad, o bien al adoptar un perfil de usuario fraudulento para inducir en error a terceros menores de edad. En general, esta modalidad fraudulenta de asumir una identidad falsa se relaciona con la necesidad de ganar la confianza del menor y así lograr un acercamiento con el propósito de menoscabar su integridad sexual. La confianza dispensada por el menor dentro de estas circunstancias le permite al agresor obtener información sensible sobre sus gustos y preferencias.(22)

Una vez logrado este objetivo, aparece por lo general la manipulación psicológica, es decir, se genera un vínculo precario en razón de las necesidades expresas o latentes del menor de edad (reconocimiento, atención, interés, aprobación, etc.). A continuación, se ingresa en la etapa de lograr que el menor de edad acceda a compartir imágenes de su propio cuerpo vinculadas necesariamente a la esfera sexual o al intercambio de material pornográfico.

En este sentido, surgirán dudas sobre la punición cuando la conducta del sujeto se limita a solicitar fotos personales o familiares del sujeto pasivo. Al tratarse de un delito de tendencia, el comportamiento del autor debe estar orientado a satisfacer un propósito ulterior, esto es, que el menor de edad participase o realizase actos de connotación sexual (desde el envío de fotos adoptando posturas sexuales o exhibiendo parte de su anatomía más reservada hasta el abuso sexual con contacto).

Sujeto activo de este delito puede ser cualquiera. Se plantean algunos interrogantes sobre la calidad de autor cuando se trata, a su vez, de un menor de edad, por ejemplo, de diecisiete años. En nuestro caso, la responsabilidad penal plena se alcanza recién a los dieciocho años (ley 22.278), si bien existe una responsabilidad atenuada o restringida para el segmento de los menores de edad que van desde los dieciséis hasta la mayoría de edad. Por este motivo, tanto el art. 15 de la *Sexual Offences Act,* como el art. 172.2 del *Criminal Code* de Canadá reprimen al adulto, es decir, a la persona de dieciocho años. El sujeto pasivo debe ser necesariamente una

(22) Pardo Albiach, Juan, "Ciberacoso: Cyberbullying...", *op. cit.*, p. 59 y ss.

persona menor de dieciocho años. En este último aspecto nuestra legislación se aparta de manera ostensible de otras regulaciones análogas, en especial, nos referimos al art. 183 *bis* del Código Penal español que prevé como sujeto pasivo a un menor de trece años.

c. La finalidad que persigue el autor

Es un delito doloso, compatible con el dolo directo. El art. 131 demanda que el autor haya realizado la conducta con el propósito específico de que el menor de edad llevase adelante actos de naturaleza sexual. En este aspecto, los actos de índole sexual bien pueden ser exhibiciones o disposición de material pornográfico obtenido del menor, por ejemplo, cuando se le solicitase que se desnude o muestre ciertas partes erógenas de su propio cuerpo (en el caso de una comunicación *online*). También puede acontecer que el autor le peticionase al menor de edad afectado el envío de imágenes pornográficas (en este caso, mediante el correo electrónico o cualquier otro medio de comunicación privado por las redes telemáticas).

La intermediación de los medios telemáticos ofrece también la posibilidad de que el autor incurra en error sobre la edad del sujeto pasivo, ya que bien puede suceder que el propio menor de edad haya falseado su propia edad para participar de chat-rooms. En este caso, debe aplicarse el error de tipo sobre la edad del sujeto pasivo y así declarar impune dicha conducta. En cambio, el art. 227-22-1 del Código Penal francés se adelanta a esta circunstancia y regula como punible también dicho contacto telemático entre el autor y la persona que se presentase como menor de quince años.

Si como consecuencia del contacto telemático, el autor lograse que el menor de edad le remitiese fotos personales de naturaleza pornográfica, las que luego son utilizados para coaccionar a la víctima y así consumar un contacto sexual (arts. 149 *bis*, 149 *ter* y 119 del Código Penal argentino), estos delitos concurren de manera material con el art. 131 CP. Como dijimos anteriormente, este delito es la antesala para la preparación de la ejecución de delitos sexuales con contacto personal con el menor afectado. En este sentido, el citado art. 227-22-1 del Código Penal francés reprime como agravante la circunstancia de que el autor se haya encontrado personalmente con el menor de quince años.

Tampoco la regulación de esta figura de contacto abusivo con menores de edad ha sido exitosa en este terreno. En la legislación comparada, en especial el art. 183 *bis* del Cód. Penal español, se ha determinado cuáles serían los actos con connotación sexual. Del modo en que está regulado en nuestro Código Penal, resulta excesivamente amplia dicha tendencia subjetiva del autor. En este punto, debemos analizar de manera hermenéutica la actual regulación de los delitos sexuales y así comprender que el medio utilizado (Internet) condiciona en gran medida la capacidad de acción del autor. En este caso, el autor debería exigirle a la víctima menor de edad que realizase desnudos, poses o directamente actos sexuales (masturbación, juegos eróticos, autorreferentes o con terceros). Los demandados "actos con connotación sexual" ciertamente incluyen por exceso a todos los actos mencionados, pero podría suceder que el autor de esta clase de delitos sexuales emplease otros medios indirectos para lograr la confianza de la víctima y así le solicitase el envío de fotografías personales para conocerla o alabar su belleza u otras cualidades físicas de la persona contactada. En este caso, dicha conducta de solicitar fotos personales de la víctima se enrola en el sendero de ganar su confianza para luego, por medio de la seducción o engaño, convencerla de que las imágenes personales vayan adquiriendo otra naturaleza. El primer segmento de la conducta sería, a nuestro juicio, atípico, ya que el envío de imágenes personales no alcanza para calificarlas de "imágenes pornográficas" con arreglo al alcance determinado por el propio art. 131 CP.

Este delito de tendencia ha sido objetado respecto de los aspectos procesales de su correcta comprobación. Puede suceder que nuestro autor se contactase con el menor de edad bajo el uso de un seudónimo y suministrando datos personales falsos, en especial nos parece importante acá subrayar la edad y el uso impostado de términos, expresiones o modismos, como temas exclusivamente relacionados con el ambiente del menor para lograr un encuentro personal. En estos casos, se presentan serios problemas para poder tipificar esta conducta como punible. Problemas parecidos han surgido en otros ordenamientos penales en torno de la delimitación de este comportamiento de otro impune, ya que la intencionalidad del autor juega un papel significativo para determinar la lesividad de dicho comportamiento.

Respecto de la consumación, este comportamiento se consuma cuando el autor determina a la víctima menor de edad a realizar los actos de natu-

raleza sexual. No se requiere que efectivamente dichos actos sexuales se hayan materializado, tan sólo que se encuentren presentes los extremos objetivos y subjetivos exigidos por esta figura. El simple falseamiento de datos personales en la red telemática no es suficiente para tener por intentado este delito. Tampoco lo es el simple contacto comunicacional con el menor de edad bajo este contexto. Lo determinante para poder hablar de un principio de ejecución será que el autor haya ejercido alguna influencia sobre el menor para lograr su lasciva finalidad. Cuando el autor orienta el giro del contacto telemático con la víctima sobre su actividad sexual, preferencias, costumbres o directamente realiza una propuesta o envía material pornográfico, entendemos que ha superado en ese supuesto el umbral de la tentativa.

En caso del envío de material pornográfico al usuario menor de edad, esta figura podrá concurrir con la figura de facilitación o distribución de ese material prevista por el art. 128 CP.

3 | *Estatuto da Criança e do Adolescente* (art. 241-D, lei 8069/90)

3.1 | Breve análisis comparativo

En el derecho penal brasileño, el art. 241-D de la lei 8069/90 establece que tipifica delito "*Aliciar, asediar, instigar ou constranger, por qualquer meio de comunicação, criança, com o fim de com ela practicar ato libidinoso*". Las penas previstas para esta infracción son de uno a tres años de reclusión y la de multa.

A diferencia de nuestro art. 131, las conductas prohibidas exceden el mero contacto telemático, ya que se requiere el empleo del medio coactivo ("*asediar*" o *"constranger"*) o bien cierto abuso de superioridad o preeminencia sobre el menor ("*aliciar*" o *"asediar"*). Si el término "*aliciar*" se identifica con la conducta de seducir a otro, se aproxima más a la naturaleza de este delito sexual. En este aspecto, la ley brasileña presenta una amplia ventaja sobre su homónima argentina ya que la barrera de punición de la primera coincide, al menos, con el ejercicio de violencia psíquica sobre el menor de edad, o el abuso de una relación de preeminencia sobre el menor en función de la mayoría de edad.

Como analizamos oportunamente, el *child grooming* se caracteriza por el empleo de medios fraudulentos, en especial, el enmascaramiento del perfil real del usuario para ganar la confianza del menor y luego pasar a la etapa de la agresión sexual. En el caso del derecho penal brasileño, se ha optado por la tipificación de conductas que atentan contra la indemnidad del menor de edad de un modo directo, esto es, con el uso de violencia o abuso intimidatorio, no se requiere en ningún caso el engaño o la seducción como medios típicos de comisión de este delito.

La conducta de "instigar" o "inducir" puede presentar algunos inconvenientes en su correcta interpretación en este contexto de delincuencia sexual, ya que si el menor es el que propone algún tipo de contacto o acercamiento con el usuario, cae por su propio peso la posibilidad de punir esta modalidad de comportamiento (*omnimodo facturus*). Por lo demás, en un análisis sistemático del uso del término "instigar", el autor debería crear la resolución de mantener algún contacto sexual con la víctima, pero en muchos casos los ciberacosadores no actúan de esta manera, sino que prefieren un contacto personal para conocerse, sin que el acto sexual haya sido explicitado.

En cuanto al medio utilizado, tanto la ley argentina como la brasileña engloban en la materia de prohibición a los medios de telecomunicaciones o telemáticos, pero se deja de lado los contactos personales entre el autor y la víctima. Suelen ser más que frecuentes los actos de acercamiento personal, incluso de hostigamiento a la víctima, con el propósito de mantener un contacto sexual con ella.

El art. 241-D del *Estatuto da Criança* se trata de un delito de tendencia, ya que el autor debe requerir al menor la práctica de un acto libidinoso. Nuestra ley penal exige, como vimos, que dicha tendencia se cristalice en un acto de naturaleza sexual. También criticamos dicha conceptualización por imprecisa, ya que debería haberse detallado al menos cuáles actos serían los que la ley reprime. Esta observación crítica puede hacerse extensiva a la regulación brasileña que peca en este sentido de una desmesurada amplitud. En este tópico, el art. 241-E de la misma ley bien podría brindar una solución a este problema de ambigüedad, ya que ese precepto define el contenido y alcance del acto sexual explícito o pornográfico al decir que "comprende cualquier situación que involucre a un menor o adolescente en actividades sexuales explícitas, reales o

simuladas, o en la exhibición de los órganos genitales de una menor o un adolescente con fines primordialmente sexuales".[23]

Un déficit normativo de ambos ordenamientos penales consiste en la falta de regulación de la intermediación de un tercero menor de edad. Puede suceder que el adulto utilice a un menor de edad para la comisión de este delito,[24] incluso que dicho menor participe activa y voluntariamente con el adulto para materializar los contactos telemáticos. Más allá de la eventual solución normativa que se presenta al recurrir al expediente de la autoría mediata, o directamente a la aplicación de las reglas de la participación (inducción), lo cierto es que correspondería una regulación que se acomode más a los tiempos modernos que nos tocan vivir.

4 | Epílogo

La realidad nos demuestra que los medios telemáticos pueden ser empleados para cometer delitos sexuales contra menores de edad. En este rumbo, el actual art. 131 del Código Penal argentino y el art. 241-D de la lei 8069/90 brasileña tienen la finalidad de incrementar la tutela penal de los menores de edad mediante la represión del contacto de adultos con aquellos mediante ese medio de comunicación con el propósito de atentar contra su integridad sexual. En el caso argentino, la técnica legislativa empleada no ha sido la más acertada ni la más depurada en comparación con otras regulaciones en la materia, ya que los contornos normativos de la materia de prohibición aparecen difusos, en especial en su relación con el bien jurídico tutelado, y el fuerte acento puesto en la finalidad ulterior del autor alientan una excesiva criminalización de actos preparatorios, transformando a esta nueva figura en un auténtico delito de sospecha.

Por el contrario, la ley penal brasileña tiene la ventaja de aminorar el estado de incertidumbre sobre las conductas que integran la materia de prohibición, pero tampoco logra captar en su esencia última esta moda-

(23) *"Para efeito dos crimes previstos nesta Lei, a expressão cena de sexo explícito ou pornografía compreende qualquier situação que envolva criança ou adolescente em atividades sexualis explícitas, reais ou simuladas, ou exibição dos òrgãos genitalis de uma criança ou adolescente para fins primordialmente sexuais" (art. 241-E, lei 8069/90).*

(24) Pardo Albiach, Juan, "Ciberacoso: Cyberbullying...", *op. cit.*, p. 58. Este autor refiere que la participación de menores de edad en calidad de autores no es un hecho extraño o aislado.

lidad de conducta fraudulenta. Decimos esto, porque el término "*aliciar*" se ajusta con la conducta de seducción que asume el autor de este delito, pero está ausente el medio engañoso o fraudulento que ha caracterizado por siempre a esta infracción. En general, los medios coactivos han sido regulados como formas de agravación de lo injusto típico de este delito (art. 183 *bis in fine*, Código Penal español).

En síntesis, las críticas apuntadas pretenden subrayar los déficits en la regulación de esta forma de criminalidad sexual informatizada y así que la necesidad político-criminal de su punición sea homogenizada a los estándares constitucionales y los principios del derecho penal que rigen la materia, en especial, los de lesividad y mínima intervención.[25]

(25) Silva Sánchez, Jesús, *Aproximación al derecho penal contemporáneo*, 2ª ed., Maestros del Derecho Penal, Nª 31, Gonzalo D. Fernández (director), Gustavo Eduardo Aboso (coord.), BdeF, Bs. As.-Montevideo, 2010, pp. 393 y ss. / 424 y ss.; Morillas Cuevas, Lorenzo "Nuevas tendencias del derecho penal. Una reflexión dirigida a la cibercriminalidad", en *Cuadernos de Política Criminal*, nº 94, 2008, pp. 5 y ss. / pp. 31 y ss.

Aspectos dogmáticos del *grooming* legislado en Argentina

por **GUSTAVO E. L. GARIBALDI**[1]

I | Introducción

En el presente me propongo enumerar algunas de las recomendaciones que la Asociación Internacional de Derecho Penal —en adelante, AIDP— formula para legislar delitos vinculados a las tecnologías de la comunicación, tanto en sus aspectos dogmáticos como de técnica legislativa y respuesta punitiva. Luego, analizaré la ley argentina en cuanto a la figura que prohíbe bajo amenaza de pena contactar a menores de edad a través de ciertos medios con el propósito de cometer algún delito contra su integridad sexual. También mostraré los problemas dogmáticos que presenta la regulación, así como notables diferencias con otras legislaciones que contemplan análoga cuestión.

Finalmente, argumentaré que el art. 131 CP, conforme el texto ordenado por la ley 26.904 (BO 11/12/2013), no cumple con los estándares recomendados y que no es compatible con premisas de orden constitucional sin un relevante esfuerzo de interpretación.

(1) Doctor de la UBA en el Área de Derecho Penal. Profesor Regular de Derecho Penal y Procesal Penal de la UBA. Profesor de la Maestría en Derecho de la Universidad de Palermo. Profesor Invitado de la Universidad Federal de Minas Gerais (Brasil). Juez en lo Criminal de un Tribunal de San Martín, Provincia de Bs. As.

2 | Recomendaciones de la AIDP

Las recomendaciones de la AIDP que me interesa puntualizar se pueden sintetizar del siguiente modo:

- Los delitos, en el ámbito de las tecnologías de la información y la comunicación (TIC) y el ciberespacio, deben ser **definidos por la ley**.
- La ley debe emplear términos que **definan la conducta prohibida de la manera más precisa posible.**
- Son **legítimas** las leyes que deciden **penalizar actos preparatorios** (de ataques a intereses relativos a las TIC y al ciberespacio) siempre **que creen un riesgo de causar un daño o peligro concreto** a intereses protegidos de otros.
- Cuando se castiguen los actos preparatorios **la pena debería ser menor.**
- Si un Estado decide criminalizar la **conducta de hacerse pasar por personas inexistentes** debe limitarse a los actos cometidos **con la intención de causar daño.**
- Se pone especial **énfasis** en conductas vinculadas a la **pornografía infantil**, aunque también en ese caso se establece alguna clase de **límite,** puntualizando el caso en que se implican niños reales.

3 | Especie de delito sancionado en Argentina mediante la ley 26.904

El art. 131 CP, texto vigente desde los últimos días del 2013, dice: "Será penado con prisión de seis (6) meses a cuatro (4) años el que, por medio de comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos, **contactare** a una persona **menor** de edad, **con el propósito** de cometer cualquier delito contra la integridad sexual de la misma".

En el 2008, Argentina sancionó la ley 26.388 y adaptó su legislación al "Convenio sobre Cibercriminalidad" realizado en Budapest en el año 2001. Luego, adhirió al mencionado Convenio. En el ámbito de la Unión Europea fue surgiendo también interés en la incorporación de otros tipos legales y es en ese marco que se puede mencionar el *grooming*.

El vocablo inglés *groom* se refiere a preparación o acicalamiento de algo. En la pedofilia, se asocia con acciones que tienen por objeto socavar mo-

ral o psicológicamente a un niño para conseguir su control emocional y luego, su abuso sexual.[2]

La doctrina ha clasificado los delitos informáticos según el **objeto de protección**. Si el "bien jurídico afectado se relaciona con los datos o información automatizada" a la que se accede de modo no autorizado, los llama **propios.** En cambio, son **impropios** aquellos en los que la informática es utilizada como medio para la comisión de un delito distinto de aquel de acceso no autorizado.[3]

La simple lectura de la ley argentina permite advertir que **las comunicaciones electrónicas, telecomunicaciones y tecnologías de transmisión de datos son la modalidad prevista de comisión del delito**. Quien se contacta **personalmente** con un menor con el mismo propósito no realiza una conducta típica.

La informática y otros medios de comunicación a distancia son así: el medio comisivo de una conducta que no tiende a la afectación de datos o información automatizada (delitos informáticos propios) y que tampoco es el medio para la comisión de otro delito no se adecua a la clasificación, porque el delito se puede cometer únicamente a través de los medios que enumera la ley; el medio define la conducta criminal.

4 | El comienzo de ejecución de los delitos informáticos

Son suficientemente conocidas dentro de la teoría de la tentativa las cuatro etapas que se distinguen: **ideación**, **preparación**, **tentativa** y **consumación**. El punto clave de ese camino que delimita lo punible es el llamado

(2) Ver Riquert, M., *Código Penal Comentado de Acceso Libre, Asociación Pensamiento Penal,* [en línea] http://www.pensamientopenal.com.ar

(3) Así, Vianna también incluye en la clasificación **delitos informáticos mixtos** y **delitos informáticos mediatos o indirectos**. Los primeros, delitos en donde, además de la protección de la inviolabilidad de datos, la norma tutela un bien relevante de otra naturaleza (se ejemplifica con el acceso no autorizado a sistemas del servicio electoral). Los **delitos mediatos o indirectos** no son informáticos, sino que heredan esa característica del medio que posibilita la consumación (por ejemplo, el acceso ilegal al sistema de un banco para transferir dinero a cierta cuenta). Véase Vianna, T., "*Fundamentos de Direito Penal Informático*", 1ª ed., Río de Janeiro, Forense, 2003. Para otras clasificaciones, Palazzi, P. A., *Delitos Informáticos*, Bs. As., Ad-Hoc, 2000, pp. 39/47.

comienzo de ejecución. Se trata de un principio garantista, recibido en gran número de códigos penales que lo mantienen. Dado que la tentativa solo existe cuando se comienza la ejecución del delito queda excluida la fase de **deliberación interna** y se consideran punibles como tentativa únicamente los **actos externos**.[4]

Del principio de ejecución también es posible extraer que no todos los actos externos pueden ser considerados tentativa. Esa fase de la conducta punible se reserva a aquellos dirigidos a la realización del delito. De esta manera, los actos preparatorios son impunes, a menos que el legislador determine lo contrario. En todo caso, se trata de excepciones al principio general de impunidad de la preparación.[5]

Las ideas de la Revolución Francesa aplicadas a esta cuestión revelan la constante preocupación del liberalismo por defender al individuo frente al poder del Estado; una distinción entre **Moral y Derecho,** que mantiene a la moral en la esfera interna del individuo y reserva el derecho a los actos exteriores, encaminados a la realización delictiva. También exige limitar la punición de actos ejecutivos a aquellos más próximos a la consumación del delito, excluyendo los que por su lejanía pudiesen dar lugar a la arbitrariedad e inseguridad jurídica.[6]

La garantía se consolidó en Alemania en la primera mitad del siglo XIX, reemplazando —al menos parcialmente— la base que representaba la *Constitutio Criminalis Carolina,* hija de los juristas italianos de la Edad Media y sus fuentes romanas. Hasta entonces, se había considerado tentativa toda manifestación exteriorizada de voluntad, dirigida a la realización del delito, y luego se consideraban punibles las acciones preparatorias. Exteriorizar la voluntad delictiva ya era delictivo: Köstlin, por ejemplo, reprochaba a Mittermaier haberse dejado seducir por el derecho francés.[7]

(4) Ver Farré Trepat, E., *La tentativa del delito,* Barcelona, Bosch, 1986, p. 138.

(5) Farré Trepat, E., *ibid.,* pp. 138/139.

(6) *Ibid.,* p. 140.

(7) *Ibid.,* p. 142.

El Código Penal argentino recibe el principio vinculado al de legalidad constitucional al definir la tentativa como realización de aquel que "con el fin de cometer un delito determinado *comienza su ejecución*, pero no lo consuma por circunstancias ajenas a su voluntad…" (art. 42 CP).

Los **delitos informáticos propios** permiten distinguir fases. Es claro que no puede ser punida la **ideación** (*cogitationis poenam nemo patitur);*[8] así, el problema remite a la etapa de preparación de un acceso no autorizado.

Tal **preparación** comienza con la recolección de información sobre el objeto del ataque. El agente traza un perfil del sistema de la víctima (*footprint*), que le permitirá un ataque exitosamente dirigido.[9] Dentro de la preparación, certifica luego los sistemas activos que se pueden alcanzar por Internet. Se trata de una fase de barrido que procura determinar las puertas de acceso y sistema operacional en uso.[10] Evalúa así a la víctima y las probabilidades de éxito del ataque, de modo equiparable al merodeo e inteligencia previa de cualquier delito.

La última fase preparatoria es de enumeración y determinación de fragilidades de la víctima, que consiste en la identificación de las cuentas válidas de usuarios y de los recursos mal protegidos.[11] Luego, el descubrimiento de contraseñas o identificación de puntos débiles es simplemente cuestión de tiempo. El **comienzo de la ejecución** y la **consumación** requieren el **acceso** a los datos y su **lectura** o ejecución.[12]

Los **delitos informáticos impropios** comienzan su ejecución cuando tiene inicio la infracción respecto de la que el sistema informático es un medio. He mostrado que en el caso de la ley argentina solo a través de ciertos sistemas de comunicación (electrónico, telecomunicaciones u otra tecno-

(8) Ver Ulpiano, 18 Dig. 48, 19 (citado por H. Mayer en JZ, 1949, p. 174).

(9) Ver Vianna, T., *op. cit.*, pp. 69/73 (*v. gr.* dominio, dirección IP, mecanismos y listas de control de acceso, nombres de usuarios). Rosende admite también la tentativa aplicable a delitos informáticos (Rosende, E., *Derecho Penal e Informática. Especial referencia a las amenazas lógico informáticas*, Bs. As., Fabián J. Di Plácido Editor, 2007, p. 308).

(10) *Ibíd.*

(11) *Ibíd.*

(12) *Ibíd.*

logía de transmisión de datos) se puede dar inicio a un intento de **contacto** típico. Pero además, bastaría con comenzar a contactarse, una acción que solo la buena interpretación permitirá no alejar desmedidamente del efectivo contacto. En cualquier caso, resulta extraño y poco razonable.

De por sí es problemático especificar cuáles son las características definitorias de una figura legal donde intervienen elementos valorativos, así como también una descripción que sea análoga a la propia definición. Las acciones pueden describirse de distintas maneras, en atención a las propiedades empíricas que presentan e incluyen en la descripción. En cualquier caso, aparecerá el problema de la indeterminación del lenguaje natural.(13)

No se contacta ni se intenta contactar —en un sentido típico— sino quien lo hace con cierta desvalorada ultra-intención. Se contacta y lo intenta quien se contacta o intenta contactar, vale decir, quien establece o intenta establecer contacto o comunicación con un menor de edad.(14)

De esta manera: ¿intenta contactarse quien simplemente llama a quien no atiende por estar ocupado en ese momento?; ¿se contacta quien es atendido, pero no recibe respuesta?; ¿desiste voluntariamente quien no responde a quien atiende o en ese caso, ni se contacta, ni intenta contactarse?

Cualquier modalidad planificada de *grooming* incluye, probablemente, varias fases. Es razonable pensar en la generación de un lazo de amistad con el menor, frecuentemente, fingiendo ser un niño o una niña. Luego, la obtención de información del menor, preparando la fase de **afectación.** Una etapa que incluye la **seducción,** procurando conductas con significado sexual y quizá, finalmente, la **extorsión** para hacerse de pornografía o lograr contacto físico prohibido. Un complejo de conductas equiparable, en cierta forma, a la descripción realizada para los delitos informáticos en sentido estricto o propio, donde en todo caso **la seducción en busca de ciertas conductas se equipara al acceso a los datos en los delitos propiamente informáticos.**

Simplificado por una única acción consistente en **contactar** (por cierto medio y con cierta inconfesable finalidad), ni siquiera permite su adecuación

(13) Ver Guarinoni, R., *Derecho, lenguaje y lógica*, Bs. As., Lexis-Nexis, 2006, p. 69.

(14) "Contactar: Establecer contacto o comunicación con alguien" (ver Real Academia Española, Diccionario de la lengua española, 22ª ed., 2001 [en línea], http://www.rae.es/)

a la especie de delito informático impropio. Se sanciona la realización de un acto que, cometido personalmente, sería preparatorio de alguna de las especies tradicionalmente legisladas para reprimir afectaciones contra la integridad sexual. Pero además, teniendo en cuenta sus orígenes, se legisla el *grooming* previendo su consumación, cuando no hay preparación ni acicalamiento ni acción alguna que tienda a socavar moral o psicológicamente al menor.

Chiara Díaz dice que en el art. 131 CP "se ubicó la figura de hacer proposiciones a niños con fines sexuales",[15] al considerarse insuficiente para la protección de niños y jóvenes la producción, ofrecimiento, difusión o posesión de pornografía infantil por medio de un sistema informático. Explica que se tuvieron en cuenta, especialmente, las facilidades para enmascarar identidades, crear otras y mantener el anonimato en redes sociales cibernéticas. Una tipificación poco precisa, a su juicio, conseguía márgenes de impunidad respecto de afectaciones a la integridad sexual de los menores que eran inicio al camino del acoso cibernético. Elogia así que, con auxilio de antecedentes extranjeros notables y la opinión de expertos en la materia, se haya adelantado la franja de punición para comportamientos anteriores a delitos más graves.[16] Llama la atención el elogio.

La figura legislada no consiste en "hacer proposiciones a niños", ya que por lo pronto no lo son todos los menores de 18 años. Además, **contactar con cierto propósito** no equivale a proponer.

Si algo cabe decir de la tipificación es que ahora estamos frente a una **específicamente** poco precisa descripción que no solo admite perseguir acciones ciertamente alejadas del acoso cibernético, sino también de cualquier afectación razonablemente delictiva de la integridad sexual.

Llama menos la atención cuando también se lee:

> "… se ha logrado un producto legislativo idóneo para afrontar situaciones de desvirtuación de los sistemas informáticos con el objetivo preciso de incrementar la protección de niños y jó-

(15) Chiara Díaz, C. A., "Incorporación del *grooming* al Código Penal Argentino" [en línea] elDial.com - CC37BB

(16) Chiara Díaz, C. A., *ibid.*

> venes, específicamente de las redes de trata y de pederastas inescrupulosos que hasta ahora han contado con facilidades para conseguirlo a fin de satisfacer sus propios vicios, lo que obviamente nos parece positivo".[17]

Algo así como, "la ley es adecuada porque va a permitir perseguir a gente mala que hasta aquí, no podía ser perseguida".

El fortalecimiento doctrinario de cualquier decisión o propuesta vinculada a la legislación represiva exige, primero, una legitimación positiva. Restar facilidades a los pederastas —escrupulosos o no— puede ser un objetivo deseable, pero la validación de la amenaza y la sanción penal exigen la configuración de una conducta que se esté facultado a prohibir, convirtiéndola en delito. Solo entonces podrá ser cometido por un infractor penal.

5 | Otras legislaciones: Chile y España[18]

A diferencia de la ley argentina, el **Código Penal de Chile** regula la cuestión en el art. 366 *quater* de modo bien diferente.[19] Por de pronto, la regla general no incluye el uso de cierto medio de comunicación, sino que el empleo de cualquier medio electrónico se equipara con la realización personal. Así, se sancionan las siguientes conductas:

- Quien para procurar excitación sexual realiza acciones de significado sexual ante un menor de 14 años, lo hace ver o escuchar pornografía.
- Quien, para el mismo fin, determina al menor a realizar tales acciones.
- Quien lo hace con un menor de más de 14 años mediante amenazas.

(17) *Ibid.*

(18) En el trabajo ya citado de Riquert se pueden consultar las legislaciones de Brasil y Perú, además de España (Ver Riquert, M., *op. cit.*, pp. 10/11).

(19) Art. 366 *quater:* "el que, sin realizar una acción sexual en los términos anteriores, para procurar su excitación sexual o la excitación sexual de otro, realizare acciones de significación sexual ante una persona menor de catorce años, la hiciere ver o escuchar material pornográfico o presenciar espectáculos del mismo carácter, será castigado con presidio menor en su grado medio a máximo. Si, para el mismo fin de procurar su excitación sexual o la excitación sexual de otro, determinare a una persona menor de catorce años a realizar acciones de significación sexual delante suyo o de otro, la pena será presidio menor en su grado máximo. Con iguales penas se sancionará a quien realice alguna de las conductas

Luego, prevé que las penas se aplicarán cuando tales conductas se cometen a distancia mediante el empleo de cualquier medio electrónico. Finalmente, la respuesta punitiva es más severa si se falsea la identidad o la edad.

También es posible puntualizar otras diferencias relevantes. Se establece la edad de 14 años para diferenciar la mayor o menor gravedad de las conductas prohibidas, exigiéndose la realización de amenazas en los casos de mayores de esa edad. Se especifica que las conductas prohibidas consisten en la propia realización de acciones de significado sexual ante el menor, la exhibición gráfica o auditiva de pornografía y la determinación para que el menor realice tales acciones. Se agrava la pena si se simula cierta edad o identidad.

Por su parte, el **Código Penal español** en el art. 183 *bis*[20] prevé una fórmula que, con una estructura inicialmente similar a la Argentina respecto de los medios de comisión, es ciertamente más compleja para caracterizar la conducta típica.

A través de comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos y con el fin de cometer agresiones, abusos y ciertas exhibiciones sexuales, se exige: contactar a un menor de 13 años y proponerle concertar un encuentro, siempre que se acompañe la propuesta de actos materiales encaminados al acercamiento. Luego, califica la figura si se obtiene el acercamiento mediante coacción, intimidación o engaño.

De nuevo, las diferencias son evidentes. Contactar y proponer concertar un encuentro, acompañando la propuesta de actos dirigidos a lograr el

descritas en los incisos anteriores con una persona menor de edad pero mayor de catorce años, concurriendo cualquiera de las circunstancias del numerando 1° del art. 361 o de las enumeradas en el art. 363" (ver ley 19.927, fecha publicación: 14/01/2004).

(20) Art. 183 *bis*: "el que a través de internet, del teléfono o de cualquier otra tecnología de la información y la comunicación contacte con un menor de trece años y proponga concertar un encuentro con el mismo a fin de cometer cualquiera de los delitos descritos en los arts. 178 a 183 y 189, siempre que tal propuesta se acompañe de actos materiales encaminados al acercamiento, será castigado con la pena de uno a tres años de prisión o multa de doce a veinticuatro meses, sin perjuicio de las penas correspondientes a los delitos en su caso cometidos. Las penas se impondrán en su mitad superior cuando el acercamiento se obtenga mediante coacción, intimidación o engaño" (ref. BOE-A-1996-4943).

acercamiento es bien distinto de contactar con cierta ultraintención. Luego, ni siquiera es ese el principio y fin de toda la regulación española: El menor no debe haber cumplido 13 años y el delito es más grave si media coacción, intimidación o engaño.

Nada fue previsto por el legislador argentino que, en consecuencia, convirtió en aparentemente delictivo todo intento de contacto malintencionado con un menor de 18 años, ya sea utilizando el teléfono o la computadora.

Por último, los tipos penales que no pueden ser sino conductas antijurídicas echan por tierra buena parte de la elaboración y distinciones racionales que propone la dogmática penal. No es posible concebir en la descripción seleccionada la concurrencia de causas de justificación. El **contacto** o su intento, acompañados del **desaprobado propósito,** difícilmente puedan ser concebidos, siquiera en hipótesis, como conductas justificadas.

6 | ¿Por qué se legisló de este modo?

Ya en 2008, en el marco de una jornada sobre delitos informáticos, se puso énfasis en que era necesaria la regulación de las conductas conocidas como *grooming*.[21]

El Proyecto presentado en 2010 procuraba la introducción en el Código Penal argentino del art. 125 *ter.* Si bien la pena propuesta era sensiblemente mayor a la del art. 131 finalmente sancionado, la conducta prevista suponía la creación de un riesgo cuya legitimidad era ciertamente menos cuestionable.

Se refería a quien "… utilizando medios electrónicos, **perturbare moral y/o psicológicamente** a menores de dieciocho años **con fines de someterlos sexualmente** mediante la utilización de transferencia de datos en cualquiera de sus formas digitales".[22]

(21) En los "Fundamentos" que acompañan la iniciativa presentada como Proyecto de Ley por la senadora nacional María José Bongiorno el 23/09/2010.

(22) Senado de la Nación, Dirección de Mesa de Entradas, 23/09/2010, exp. 5, n° 3267/10, hora 18.30.

Entre los fundamentos del Proyecto, se leen referencias a los cambios que acompañan el surgimiento de la **Sociedad de la Información**, producto de las TIC, frente a la especial situación de vulnerabilidad en que se encuentran los menores de edad. Se describe allí una realidad en la que el anonimato y la creación de identidades alternativas permiten la participación en redes sociales de "pervertidos"[23] que realizan conductas que se estiman no adecuadamente contempladas. Recomienda entonces "una tipificación clara que no deje márgenes de impunidad interpretativa ante una conducta típica, antijurídica que le sea reprochable al autor".[24]

El contenido de la discusión parlamentaria mantenida en la Novena Sesión Ordinaria del Senado de la Nación del 13/11/2013, que finalmente por unanimidad en esa Cámara convierte en ley al texto del actual art. 131 CP, merece un análisis puntual.

La senadora Escudero explica que el Senado había aprobado el 28/09/2011 el Proyecto que vuelve modificado de la Cámara de Diputados de modo que "desfigura completamente la sanción del Senado". El Proyecto aprobado por el Senado intentaba "alcanzar con la sanción penal conductas que hoy no están tipificadas, la captación de menores a través de la red con la intención, justamente, de cometer contra ellos un delito contra la integridad sexual". La Cámara de Diputados, en cambio, tipificó un delito distinto y modificó la pena que el Senado había propuesto, en principio, de seis meses a cuatro años de prisión.

Los cambios introducidos por la Cámara Baja eran los siguientes:

- La escala penal fue reducida, de dos meses a dos años de prisión.
- El delito pasó a ser de acción privada.
- Hizo distinción según si la víctima tuviese más o menos de 13 años de edad.
- Exigió que a través de Internet se hubieran mandado imágenes explícitas o actos de connotación sexual y que mediara engaño, abuso de autoridad o intimidación.

(23) En los "Fundamentos" de la senadora nacional María José Bongiorno ya referidos.

(24) *Ibid.*

La crítica de la Senadora fue la siguiente:

> "Nosotros queremos proteger a todos los menores porque es justamente entre la edad de 13 y 16 años cuando los chicos están más conectados en la red y donde son más vulnerables. Porque a través del anonimato que brindan las redes sociales lo que vemos es que hay muchos pederastas y redes de trata que captan a estos menores haciendo que el menor genere una relación de confianza con este delincuente y así, después vayan propiciando un encuentro donde seguramente abusarán de estos menores".

Sugiere entonces que el Senado insista con la mayoría correspondiente en la sanción original y recuerda que el origen fueron los proyectos de las senadoras Bongiorno e Higonet.

Por su parte, la senadora Bongiorno dijo que en 2010 presentó un proyecto inicial y luego los senadores Higonet y Verna en 2011 aportaron un nuevo proyecto. Se hizo una unión entre ambos y trabajaron en comisión con legislación comparada, con asesoramiento en **delitos informáticos,** concluyeron en el Proyecto aprobado en esa Cámara. A continuación, lo proponen nuevamente "más allá de la modificación de la Cámara de Diputados que (…) desvirtúa el delito, cercena las penas y (…) no corresponde a la protección integral del menor…".

La senadora Higonet dijo que coincidía con volver a su proyecto de pena mayor, que permitirá al juez adecuarla de acuerdo al **grado de delito.** Hizo referencia a un caso conocido por los medios en el que una organización en Holanda creó la imagen virtual de una niña filipina de 10 años y la expuso en los medios sociales electrónicos, a lo cual una gran cantidad de pederastas en el mundo mostraron interés. Dijo que constantemente hay 750.000 pedófilos conectados a la red y que la UNICEF informa que el treinta por ciento de los menores de entre cuatro y dieciséis años ha sufrido algún tipo de acoso, aunque solo el 7% se atreve a contarlo por temor a no poder tener acceso a Internet, destacando el daño psicológico que se les inflige.

Finalmente, revela confusión dogmática al criticar que se disminuya la pena por estar "ante la tentativa de un delito" e insiste en defensa de

su posición, la que —precisa la legisladora— pena "el *contacto* que esa persona mayor busca con un menor *a través de un medio tecnológico*, a través de internet". Uno que, a su juicio, "marca, inequívocamente, cuál es el destino que tiene ese fin, que es justamente el delito". Esto es, que el menor realice algún tipo de acción o de actividad sexual y así sea posible que comience la etapa del ciberacoso.

El senador Cano dijo que el 47% de los menores abre su primera cuenta después de los 13 años. El 20% de las chicas y el 7% de los varones afirma que una persona que conocieron por Internet —no personalmente— les pidió que le envíen fotos con poca ropa.

El senador Fernández dijo:

> "No es cuestión nuestra ponernos a evaluar qué se interpretó en la Cámara de Diputados para convertir las conductas reprochadas en conductas que significaban menos pena o cosas por el estilo. No entiendo qué significa eso de menos de trece o más de trece. No entiendo qué tiene que ver. Nosotros tenemos muy claro que lo que estamos planteando son delitos novedosos, que hablan de nuevas conductas, y que como nuevas conductas reprochadas deben ser tipificadas para que se conviertan en delito. Y en ese marco es donde nosotros queremos consolidarlo".

A continuación, se votó y por unanimidad se convirtió en ley, pese a algunas dudas, ya que la presidente en aquel momento, Rojkes de Alperovich, dijo: "Regresa a Diputados. Muy bien", pero varios senadores corrigieron: "¡No! Es ley", convirtiéndose en ley la sanción original del Senado.

De este modo, es posible observar que no todos los proyectos tuvieron el texto que finalmente se sancionó. El originario era ciertamente menos cuestionable en cuanto a la descripción de la conducta prohibida. **Perturbar** supone un curso de acción lesivo que no necesariamente revela **contactar.** La propuesta de la Cámara de Diputados exigía el envío de imágenes explícitas o la realización de actos de connotación sexual, mediando engaño, abuso de autoridad o intimidación.

Se ponía la ley argentina en línea con estándares razonables, se respetaba —se verá— la proporcionalidad de la respuesta punitiva prevista por el

Código Penal para otros delitos contra la integridad sexual y se distinguía según la edad de la víctima, en cualquier caso, en consonancia con legislaciones como las de España o Chile.

Los motivos del Senado, entonces, se pueden resumir del siguiente modo:

- La especial situación de vulnerabilidad en que se encuentran los menores de edad y con relación al *grooming* particularmente, la franja entre 13 y 16 años.
- La idea de lograr la protección integral de los menores.
- Las posibilidades de que el autor se valga del anonimato y la creación de identidades alternativas.
- La necesidad de una legislación clara que no deje márgenes de impunidad producto de la interpretación.
- La realidad de la captación de menores, generando una relación de confianza que propicia un encuentro para consumar el abuso sexual.
- El daño psicológico que se genera en los menores.
- El riesgo de que se envíen fotografías inconvenientes.

Sucede que lo que se prohíbe no es el aprovechamiento de la situación de vulnerabilidad ni valerse del anonimato o crear identidades alternativas ni la generación de una relación de confianza propiciatoria de encuentros ni la perturbación psicológica de los menores ni el envío de cierta clase de fotografías. Contactar (aun con la peor de las finalidades) es anterior a cualquiera de esas otras conductas y eso es, precisamente, poco claro. Para no dejar márgenes de impunidad a la interpretación se habilitó toda una franja propicia para la punición.

No deseo ensañarme con las afirmaciones de ningún legislador que, por cierto, puede nada saber de dogmática penal y confundir preparaciones, tentativas y escalas penales. Pero **debe quedar claro en este trabajo que no se ha prohibido bajo amenaza de pena un acto preparatorio, sino la preparación de un acto preparatorio. La preparación de la preparación.**

Finalmente, desalienta un discurso que insiste en la sanción de una ley, tras confesar que no se entiende por qué se hacen modificaciones o se proponen distinciones.

7 | Los problemas de la ley a la luz de las recomendaciones de la AIDP y ciertos principios constitucionales

Veamos ahora las recomendaciones de la AIDP y comparemos con lo legislado en Argentina.

Los delitos, en el ámbito de las TIC y el ciberespacio, deben ser definidos por la ley que debe emplear términos que definan la conducta prohibida de la manera más precisa posible.

La ley argentina ha definido el llamado delito de *grooming*, pero indudablemente lo ha hecho empleando términos que describen la conducta prohibida del modo menos preciso posible. Tal es el adelantamiento y tal la simplificación, que se produce un corrimiento del comienzo de ejecución hacia momentos que, en cualquier otro caso, remiten a una etapa bien temprana de preparación.

Son legítimas las leyes que deciden penalizar actos preparatorios (de ataques a intereses relativos a las TIC y el ciberespacio), siempre que creen riesgo de causar un daño o peligro concreto a intereses protegidos de otros.

Sin discutir aquí si la recomendación se basa en presupuestos correctos[25] desde la lógica que la informa, es posible afirmar: cuanto más alejados del daño o peligro concreto al interés que se pretende proteger estén los actos preparatorios contemplados, menos probabilidades habrá de crear efectivamente un peligro concreto o riesgo de daño para el interés protegido. Al menos, si se comparan los riesgos de un mismo curso delictivo, que progresa hacia la consecución de cierto peligro o daño.

Luego, es claro que la constelación de riesgos prohibidos que derivan de la ley argentina en análisis abarca situaciones que no causan daño ni suponen peligro concreto.

(25) Hay actos ejecutivos (tentativas punibles) que generan menor riesgo concreto para el bien protegido que ciertas conductas preparatorias impunes. Ver Sancinetti, M., "El fracaso de la explicación del ilícito de la tentativa sobre la base de un 'peligro objetivo'", en *Teoría del delito y disvalor de acción*, Bs. As., Hammurabi, 1991, pp. 360 y ss.

Cuando se castiguen los actos preparatorios la pena debería ser menor.

La pena prevista es efectivamente menor que otras muy graves que acompañan delitos contra la integridad sexual legislados en el mismo Título III del Código Penal argentino. No obstante, la recomendación tampoco se cumple en el caso del abuso sexual simple (art. 119 CP),[26] un delito de daño que prevé la misma escala penal cuando se abusa sexualmente de un menor de trece años, sin necesidad de violencia, intimidación o aprovechamiento. De modo que **contactar** por medio de cualquier tecnología a un menor que cuenta, por ejemplo, con 17 años, **con el propósito** de abusar sexualmente de él (art. 131 CP), tiene la misma respuesta punitiva que si efectivamente, se abusase simplemente de un niño de 12 años (art. 119, primer párrafo, CP).

Si un Estado decide criminalizar la conducta de hacerse pasar por personas inexistentes debe limitarse a los actos cometidos con la intención de causar daño.

La ley argentina no criminaliza la conducta de hacerse pasar por personas inexistentes, aunque su fórmula **contactare** indudablemente la abarca, entre muchas otras. Para ese contacto, efectivamente prevé el propósito de causar un daño.

Se pone especial énfasis en conductas vinculadas a la pornografía infantil.

La producción o publicación de imágenes pornográficas en que se exhibieran menores de 18 años y la organización de espectáculos en vivo con escenas pornográficas en que participaren dichos menores está sancionada en el art. 128, primer párrafo CP.[27] Una vez más, la escala penal prevista es la misma que la del art. 131 CP.

(26) Art. 119: "Será reprimido con reclusión o prisión de seis meses a cuatro años el que abusare sexualmente de persona de uno u otro sexo cuando esta fuera menor de trece años o cuando mediare violencia, amenaza, abuso coactivo o intimidatorio de una relación de dependencia, de autoridad, o de poder, o aprovechándose de que la víctima por cualquier causa no haya podido consentir libremente la acción…".

(27) Art. 128: "Será reprimido con prisión de seis (6) meses a cuatro (4) años el que produjere, financiare, ofreciere, comerciare, publicare, facilitare, divulgare o distribuyere, por cualquier medio, toda representación de un menor de dieciocho (18) años dedicado a actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales, al igual que el que organizare espectáculos en vivo de representaciones sexuales explícitas en que participaren dichos menores…".

Entonces, organizar un espectáculo con escenas pornográficas en vivo con menores (art. 128, primer párrafo CP) tiene la misma respuesta punitiva dentro de la ley penal argentina que *contactar* al mismo menor por medio de cualquier tecnología con el propósito de abusar sexualmente de él (art. 131 CP).

Estas observaciones permiten comprender, quizá, los motivos de la menor respuesta punitiva que propuso la Cámara Baja al Proyecto de ley, luego sancionado.

El principio de proporcionalidad de la penas veda el ejercicio del poder punitivo realizado de modo irracional, tal como sería una respuesta groseramente desproporcional al mal provocado.

De allí que es necesario establecer jerarquías de afectación y establecer mínima coherencia entre la magnitud de penas que se asocian a cada conflicto criminal.[28] Algo que, evidentemente, no cumple la ley Argentina.

8 | Conclusión

El art. 131 del Código Penal Argentino que contempla desde el mes de diciembre de 2013 el delito conocido como *grooming*, no respeta los estándares recomendados por la AIDP ni su propia normativa suprema vinculada con los principios de legalidad y proporcionalidad (art. 18 CN).

(28) Ver Zaffaroni, E.; Alagia, A.; Slokar, A., "Parte General" de *Derecho Penal*, Bs. As., Ediar, 2003, p. 130.

El Convenio de Budapest sobre cibercriminalidad y la Ley de Protección de los Datos Personales

por **JUAN CRUZ GONZÁLEZ ALLONCA**[1] y **EZEQUIEL PASSERON**[2]

I | Introducción

Desde hace un tiempo, el derecho informático adquirió un nuevo desafío: el **delito informático**.

La **ciberdelincuencia** es toda acción —antijurídica, típica y culpable— que tiene el objetivo de destruir y dañar ordenadores y redes por vías informáticas. Si bien las nuevas tecnologías y las conductas delictivas a ellas asociadas evolucionan velozmente, la legislación va siempre un paso atrás. De manera que muchas conductas criminales, al no estar tipificadas, no pueden considerarse delito.

Sin embargo, en el año 2008, nuestro país ha dado un paso importante en este sentido a través de la sanción de la Ley de Delitos Informáticos —26.388—, incorporando estos ilícitos al Código Penal.

(1) Director Nacional de Protección de Datos Personales en el Ministerio de Justicia y Derechos Humanos de la Nación. Abogado (UBA). Especialista en Ingeniería de Sistemas de Información (UTN). Posgrado en Gestión de la Seguridad de la Información por la Facultad de Ingeniería de la Universidad Austral. Investigador en el campo de las tecnologías para la privacidad (PET).

(2) Licenciado en Ciencias de la Comunicación (UBA). Coordinador del Programa Nacional de concientización acerca del uso responsable de las nuevas tecnologías "Con vos en la web". Desarrolla trabajos de investigación y exposiciones acerca del acceso a la información científica en la Facultad de Ciencias Sociales (UBA).

A nivel internacional, no podemos dejar de referirnos al **Convenio sobre la Ciberdelincuencia, Budapest 23/11/2001** —Convenio de Budapest—; elaborado por el Consejo de Europa en Estrasburgo, con la participación activa de los estados observadores de Canadá, Japón y China.

Éste es el primer tratado internacional que establece delitos penales cometidos a través de medios informáticos con el fin de combatir, no sólo los ciberdelitos sino, también, aquellos delitos cometidos en Internet; estableciendo reglas de cooperación internacional para que los países miembros puedan hacer frente a esta nueva delincuencia mediante la armonización de leyes nacionales y la optimización de las técnicas de investigación.

El Convenio y su Informe Explicativo fueron aprobados por el Comité de Ministros del Consejo de Europa en su 109ª reunión a principios de noviembre de 2001. A fin de mes se abrió a la firma en Budapest y entró en vigor el 1 de julio de 2004. Nuestro país fue oportuna y oficialmente invitado, por lo que actualmente se encuentra adherido al Consejo de Europa.

En caso de que su futura adhesión sea ratificada por el Congreso nacional; el tratamiento de datos personales previsto en el Convenio deberá someterse a las disposiciones de la ley 25.326, ya que éstas se aplican por principio general a todo tratamiento de datos personales.

Indudablemente, analizar el Convenio de Budapest excedería el objeto de este artículo. En esta ocasión, nos referiremos solamente a las normas que tienen relación con la protección de datos personales. Sobre todo al apartado de "Derecho Procesal" y a todas aquellas disposiciones referidas al acceso, acumulación, resguardo, análisis y, especialmente, divulgación de datos personales; para concluir si, de acuerdo a los principios regulados por la ley 25.326, constituyen una debida o indebida intromisión en la privacidad.

2 | La ley 25.326

Esta norma legal de orden público tiene por objeto la protección integral de los datos personales asentados en archivos, registros, bancos de datos u otros medios técnicos de tratamiento de datos —públicos o privados— para garantizar —de conformidad a lo establecido en el art. 43, párr. 3 de la CN— el derecho al honor y a la intimidad de las personas, y el acceso a la información que se registre sobre ellas.

A los fines de efectuar el análisis antes aludido y considerar el alcance de las disposiciones de la ley 25.326, es necesario, en primer lugar, conocer las definiciones en ella contempladas.

La referida norma legal da una serie de definiciones necesarias para considerar su alcance:

- Se entiende por **dato personal** a la información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables.
- Se entiende por **dato sensible** a la información sobre el origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual.
- Conceptos tales como **archivo**, **registro**, **base** o **banco de datos**, designan al conjunto organizado de datos personales objeto de tratamiento o procesamiento —electrónico o no—; cualquiera fuere la modalidad de su formación, almacenamiento, organización o acceso.
- **Tratamiento de datos** es un concepto que incluye a todas las operaciones y procedimientos sistemáticos —electrónicos o no— que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción, y, en general, el procesamiento de datos personales; así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias.
- El **responsable de archivo**, **registro**, **base o banco de datos** es la persona física o de existencia ideal pública o privada, titular de un archivo, registro, base o banco de datos.
- Los **datos informatizados** son aquellos datos personales sometidos al tratamiento o procesamiento electrónico o automatizado.
- El **titular de los datos** es toda persona física o persona de existencia ideal con domicilio legal, delegaciones o sucursales en el país, cuyos datos sean objeto del tratamiento al que se refiere la ley.
- El **usuario de datos** es definido como toda persona, pública o privada, que realice a su arbitrio el tratamiento de datos; ya sea en archivos, registros o bancos de datos propios o a través de su conexión.
- **La disociación de datos** es todo tratamiento de datos personales de manera que la información obtenida no pueda asociarse a persona determinada o determinable.[3]

(3) Ley 25.326, art. 2.

Para que un tratamiento de datos personales sea lícito, es requisito que el banco de datos se encuentre inscripto en el Registro Nacional de Bases de Datos habilitado por la Dirección Nacional de Protección de Datos Personales del Ministerio de Justicia y Derechos Humanos de la Nación, y se cumplan los principios de protección de datos contenidos en la citada norma legal. Esto implica, entre otras cosas, que los datos personales que se recojan a los efectos de su tratamiento deban ser ciertos, adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para los que se hubieren obtenido. Además, la recolección de datos no puede hacerse por medios desleales, fraudulentos o en forma contraria a las disposiciones de la presente ley. Tampoco pueden ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención; etc.(4)

Los datos sensibles cuentan con un régimen de mayor protección en la ley; por lo que sólo se permite su tratamiento si existe una autorización legal expresa, fundada en el interés general o cuando el tratamiento se hace con finalidades estadísticas y científicas y el titular no puede ser identificado. En la misma línea de resguardo, se establece que ninguna persona puede ser obligada a proporcionar datos sensibles. De manera que queda prohibida la formación de archivos, bancos o registros que almacenen información que directa o indirectamente revele esos datos.

No obstante, se establecen excepciones. Las autoridades públicas competentes pueden tratar los datos relativos a los antecedentes penales o contravencionales. Asimismo, la Iglesia Católica, las asociaciones religiosas y las organizaciones políticas y sindicales pueden llevar un registro de sus miembros.(5)

Por principio general, las entidades públicas no requerirán del consentimiento del titular para el tratamiento de sus datos personales; excepto cuando el tratamiento de datos pretendido exceda las atribuciones específicas del órgano administrativo. El consentimiento deberá ser libre, expreso e informado. El que se otorga para el tratamiento de los datos personales podrá ser revocado en cualquier momento, sin efectos retroac-

(4) *Ibid.*, arts. 3, 4, 21, 22 y 24.

(5) *Ibid.*, art. 7.

tivos. El carácter de informado implica que, al recabarse datos, se haga saber a su titular sobre la existencia del archivo —el nombre de su responsable y domicilio, la finalidad de la base de datos y sus destinatarios, y la posibilidad y forma de ejercer los derechos de acceso, rectificación y/o supresión con que cuenta el titular respecto de la información contenida en la base de datos—.[6]

La norma legal impone los deberes de seguridad, confidencialidad, registro y garantía a quien posea una base de datos que contenga información personal de terceros para el ejercicio de los derechos del titular del dato.[7] El responsable de la base de datos debe adoptar las medidas necesarias para garantizar la seguridad y confidencialidad de los datos personales; de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado y permitir detectar desviaciones de información —intencionales o no— provenientes de la acción humana o del medio técnico utilizado.

Asimismo, debe mantener confidencialidad de todo aquello de lo que tome conocimiento al efectuar el tratamiento de datos. Puede ser relevado de esa obligación solamente por resolución judicial y cuando medien razones de seguridad y salud públicas, y de defensa nacional.

El **deber de registro** al que nos referimos precedentemente es el que da licitud al tratamiento de datos y corresponde a toda base de datos pública o privada que exceda el uso exclusivo personal.

Finalmente, es de suma importancia garantizar, al efectuar tratamiento de datos personales, el ejercicio de los **derechos del titular del dato**: acceso, rectificación, actualización y supresión.

La ley contempla excepciones en el ejercicio de estos derechos respecto de bases públicas. Es posible que los responsables o usuarios de bancos de datos públicos denieguen el acceso, rectificación o la supresión mediante decisión fundada en función de la protección de la defensa de la Nación, del orden y la seguridad pública o de la protección de

(6) *Ibíd.*, arts. 5 y 6 y dec. 1558/01, art. 5.

(7) *Ibid.*, arts. 3, 9, 10, 14, 15, 16, 21 y 24.

los derechos e intereses de terceros; cuando se pudieren obstaculizar actuaciones judiciales o administrativas en curso, vinculadas a la investigación sobre el cumplimiento de obligaciones tributarias o previsionales; en función del desarrollo de funciones de control de la salud y del medio ambiente; la investigación de delitos penales y la verificación de infracciones administrativas. No obstante, se deberá brindar acceso a los registros en cuestión si el afectado tiene que ejercer su derecho de defensa.(8)

Hay distintos tipos de **cesiones de datos personales** por parte de los bancos de datos públicos. Las realizadas entre dependencias de la administración pública, en la medida en que sean necesarias para el cumplimiento de sus respectivas competencias, no tendrán inconvenientes si se efectúan en forma directa.

Si la cesión se efectúa al sector privado, sólo podrá hacerse de manera no masiva cuando dicha cesión se justifique con el cumplimiento del requisito del interés legítimo; previa identificación del cesionario, y siempre que se cumplan los principios de protección de datos aplicables al caso y que con dicho revelamiento no se afecte la intimidad u otro derecho de las personas.

La cesión masiva de datos personales requiere autorización de funcionario responsable. La cesión de datos sensibles sólo puede hacerse mediante autorización legal o aplicando procedimientos de disociación de la información; de modo que los titulares de los datos sean inidentificables. La cesión de datos personales genera responsabilidad solidaria de cedente y cesionario frente al organismo de control y al titular de los datos de que se trate, aunque podrá ser eximido total o parcialmente de responsabilidad si demuestra que no se le puede imputar el hecho que ha producido el daño.(9)

Es importante tener en cuenta que, para la ley 25.326, las decisiones judiciales o los actos administrativos que impliquen apreciación o valoración de conductas humanas no podrán tener como único fundamento el

(8) *Ibíd.*, art. 17.

(9) *Ibíd.*, art. 11, dec. 1558/01, art. 11.

resultado del tratamiento informatizado de datos personales que suministren una definición del perfil o personalidad del interesado. Los actos que resulten contrarios a la disposición precedente serán irrevocablemente nulos.(10)

3 | El Convenio sobre la Ciberdelincuencia

El Convenio sobre la Ciberdelincuencia (Budapest, 29/11/2001) determina que las partes adoptarán las medidas necesarias para establecer poderes y procedimientos a los efectos de investigación; o procedimientos penales específicos para ser aplicados a infracciones penales ya previstas en el Convenio, u otras de carácter informático; o para la recogida de pruebas electrónicas de cualquier infracción penal.(11)

Dichos poderes y procedimientos se aplicarán sometiéndose a las condiciones y garantías dispuestas en el derecho interno de cada estado. De manera que aseguren tanto una protección adecuada de los derechos del hombre y de las libertades, como la supervisión judicial u otras formas de supervisión independiente; teniendo siempre en miras el interés público y una buena administración de justicia.(12)

En este marco, en primer lugar, se prevé empoderar a las autoridades competentes para ordenar a una persona la **conservación** inmediata de datos electrónicos especificados —incluidos los datos de tráfico almacenados por sistema informático que permitan identificar los prestadores de servicio y la vía de comunicación utilizada— que se encuentren bajo su poder y control, manteniéndolos íntegros durante un plazo un máximo de 90 días, en el que deberá mantener el secreto de dichas medidas y luego del cual las autoridades competentes podrán obtener su revelación.(13)

(10) *Ibíd.*, art. 20.

(11) Convenio de Budapest, art. 14.

(12) *Ibíd.*, art. 15.

(13) *Ibíd.*, arts. 16 y 17.

En segundo lugar, se prevé empoderar a las autoridades competentes para ordenar a una persona **la comunicación inmediata de datos electrónicos especificados** que se encuentren bajo su poder y control —incluidos los prestadores de servicios—, almacenados en un sistema o soporte informático. La información a comunicar por los prestadores de servicios será sobre sus abonados. Puede incluir tanto datos de tráfico como de contenido —tipo de servicio de comunicación utilizado, las disposiciones técnicas adoptadas, el tiempo del servicio, la identidad, la dirección postal o geográfica, el número de teléfono del abonado o cualquier otro número de acceso, los datos relativos a la facturación y el pago—.(14)

En tercer lugar, también se prevé empoderar a las autoridades competentes para **registrar o acceder** a un sistema informático específico o soporte de almacenamiento informático específico y los datos en ellos contenidos, para decomisar, para realizar y conservar una copia de los mismos y para tomar las medidas necesarias para preservar la integridad de los datos informáticos pertinentes y para exigir a la persona que conozca el funcionamiento del sistema informático o medidas aplicadas para su protección, que proporcione todas las informaciones razonablemente necesarias para aplicar las medidas antes descriptas.(15)

En cuarto lugar, las autoridades competentes podrán **recolectar o grabar datos de tráfico e interceptar, recoger o grabar datos de contenido en tiempo real**. Podrán proceder a dicha grabación mediante un prestador de servicios en forma obligatoria o exigiendo su colaboración a las autoridades competentes para tales fines. En caso de que el ordenamiento jurídico interno de un estado no permita la grabación genérica de los datos de tráfico, debe preverse cuanto menos la grabación en tiempo real de datos de tráfico de comunicaciones específicas. El prestador de servicios debe conservar el secreto de tales operaciones e información.(16)

Por último, se prevé la **transferencia internacional de datos personales** con motivo de cooperación entre los estados firmantes con arreglo a lo dispuesto en el presente capítulo. Para ello se aplicarán los instrumentos

(14) *Ibíd.*, art. 18.

(15) *Ibíd.*, art. 19.

(16) *Ibíd.*, arts. 20 y 21.

internacionales relativos a la cooperación internacional en materia penal; acuerdos basados en la legislación uniforme o recíproca y en su propio derecho nacional, de la forma más amplia posible, con la finalidad de investigar los procedimientos concernientes a infracciones penales vinculadas a sistemas y datos informáticos o para recoger pruebas electrónicas de una infracción penal.

4 | La relación entre los cuerpos normativos

El Convenio de Budapest contiene, como se señalara precedentemente, actividades de **tratamiento de datos personales** que se encuentran expresamente contenidas en la definición efectuada por el art. 2 de la ley 25.326 y que más arriba se reprodujera.

Por otra parte, el art. 7 del mismo cuerpo legal dispone que los datos relativos a antecedentes penales o contravencionales sólo pueden ser objeto de tratamiento por parte de las autoridades públicas competentes, en el marco de las leyes y reglamentaciones respectivas.

Asimismo, la actividad informativa que regula el Convenio de Budapest tiene, eventualmente —en caso de participar un organismo policial o de inteligencia—, una previsión específica en el art. 23 de la ley 25.326. Ésta determina que el tratamiento de datos personales, sin consentimiento de los afectados, con fines de defensa nacional o seguridad pública por parte de las fuerzas armadas, fuerzas de seguridad, organismos policiales o inteligencia, queda limitado a aquellos supuestos y categoría de datos que resulten necesarios para el estricto cumplimiento de las misiones legalmente asignadas a los responsables de la defensa nacional, la seguridad pública o de la represión de los delitos. Los archivos, en tales casos, deberán ser específicos y establecidos al efecto. Deben clasificarse por categorías, en función de su grado de fiabilidad. Los datos personales registrados con fines policiales se cancelarán cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento.

En virtud de lo expuesto, se desprende que la actividad informativa que regula el Convenio sobre la Cibercriminalidad, está alcanzado por las disposiciones de la ley 25.326.

5 | Compatibilidad de las normas del Convenio de Budapest frente a la ley 25.326

Como hemos visto, la Ley de Protección de los Datos Personales establece principios generales de licitud —calidad de los datos, confidencialidad y seguridad—; y regulaciones específicas para ciertos tratamientos de datos —recolección, la cesión y la transferencia internacional—, cuyo cumplimiento vamos a analizar en las disposiciones concretas de tratamiento de datos que prevé el Convenio.

Éste contempla el tratamiento informático de datos personales relativos a hechos penales y a la investigación de delitos.

En cuanto a la calidad de los datos personales, hay que considerar que deben ser "ciertos, adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para los que se hubieren obtenido" (art. 4, inc. 1, de la ley 25.326).

Ello nos obliga a analizar si los datos a tratar se encuentran afectados por alguna prohibición legal que los convierta en inadecuados o impertinentes para la finalidad pretendida.

En el presente tratamiento tenemos dos características de calidad del dato que destacar para definir su pertinencia: a) el carácter de datos penales y b) el carácter de datos pertenecientes a comunicaciones. Ambos afectan la calidad del dato.

Con respecto a la característica del dato penal, corresponde señalar que su tratamiento coincide con lo dispuesto en la ley 25.326. Pues ésta prevé expresamente que sea la autoridad competente la adjudicataria de las facultades que otorga; lo que cumpliría con el requisito del art. 7 antes mencionado, ya que los datos sólo pueden ser objeto de tratamiento por parte de las autoridades públicas competentes en el marco de las leyes y reglamentaciones respectivas.

En caso de que el dato objeto de tratamiento pertenezca al ámbito de las comunicaciones, hay que considerar el secreto legal que lo afecta. El

art. 18 de la CN dispone que "es inviolable (…) la correspondencia epistolar y los papeles privados: y una ley determinara en qué casos y con qué justificativo podrá procederse a su allanamiento y ocupación". En similar sentido el art. 19 de la Carta Magna establece que:

> "las acciones privadas de los hombres que de ningún modo ofendan al orden y a la moral pública, ni perjudiquen a un tercero, están sólo reservadas a Dios, y exentas de la autoridad de los magistrados. Ningún habitante de la Nación será obligado a hacer lo que no manda la ley, ni privado de lo que ella no prohíbe".

Por su parte, la Convención Americana de Derechos Humanos que goza de jerarquía constitucional (art. 75, inc. 22, de la CN) reconoce el derecho a la honra y a la dignidad. Establece que nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, la de su familia, en su domicilio, en su correspondencia. Del mismo modo, el Pacto Internacional de Derechos Civiles y Políticos aprobado por ley 23.313 y con la misma jerarquía constitucional, consagra el derecho a la intimidad.

En la legislación infra constitucional, la Ley de Telecomunicaciones —ley 19.798—, que rige las telecomunicaciones en el territorio de la Nación Argentina y en los lugares sometidos a su jurisdicción; define como telecomunicación a toda transmisión, emisión o recepción tanto de signos como de señales, escritos, imágenes, sonidos o informaciones de cualquier naturaleza; ya sea por hilo, radioelectricidad, medios ópticos u otros sistemas electromagnéticos.

La ley dispone la inviolabilidad de la correspondencia de telecomunicaciones. Es decir, prohíbe abrir, sustraer, interceptar, interferir, cambiar su texto, desviar su curso, publicar, usar, tratar de conocer o facilitar que otra persona que no sea su destinatario conozca la existencia o el contenido de cualquier comunicación confiada a los prestadores del servicio y la de dar ocasión de cometer tales actos. Y obliga a las personas afectadas a los servicios de telecomunicaciones y a quienes de cualquier manera tengan conocimiento de la existencia o contenido de la correspondencia de telecomunicaciones a guardar secreto respecto de su existencia y contenido. De manera que su interceptación sólo procederá a requerimiento de juez competente.

A su vez, la ley 25.520 de Inteligencia Nacional dispone que, las comunicaciones telefónicas, postales, de telégrafo o facsímil; o cualquier otro sistema de envío de objetos o transmisión de imágenes, voces o paquetes de datos; así como cualquier tipo de información, archivos, registros y/o documentos privados o de entrada o lectura no autorizada o no accesible al público; son inviolables en todo el ámbito de la República Argentina; excepto cuando mediare orden o dispensa judicial en sentido contrario. Además

> "cuando en el desarrollo de las actividades de inteligencia o contrainteligencia sea necesario realizar interceptaciones o captaciones de comunicaciones privadas de cualquier tipo, la Secretaría de Inteligencia deberá solicitar la pertinente autorización judicial. Tal autorización deberá formularse por escrito y estar fundada indicando con precisión el o los números telefónicos o direcciones electrónicas o de cualquier otro medio, cuyas comunicaciones se pretenda interceptar o captar".

De lo expuesto se infiere que, ante el secreto que afecta al dato de las comunicaciones, su tratamiento sólo puede ser dejado sin efecto de manera excepcional y por disposición legal, como indica el art. 18 de la CN.

Finalmente, cabe hacer referencia a la ley 25.873. Ésta dispuso incorporar nuevos arts. a la ley 19.798 con el fin de que todo prestador de servicios de telecomunicaciones disponga de los recursos humanos y tecnológicos necesarios para la captación y derivación de las comunicaciones que transmiten, para su observación remota a requerimiento del Poder Judicial o el Ministerio Público de conformidad con la legislación vigente; lo que incluyó la retención y cesión de datos de tráfico de las comunicaciones por el plazo de 10 años y la cesión de datos de contenido de las comunicaciones para casos determinados. Esta ley fue declarada inconstitucional, con efecto de alcance colectivo, para todos los usuarios que se encuentren en la misma condición que el actor en los autos caratulados "Halabi Ernesto c/ PEN ley 25.873 - decreto 1563/04 s/ amparo ley 16.986", de fecha 29/11/ 2005.

Al quedar firme la sentencia de Cámara, podemos decir que se ha sellado la ineficacia de dicha normativa. En dicho fallo, la Cámara Nacional de Apelaciones en lo Contencioso Administrativo Federal, Sala 2ª, exige que

la eventual norma que permita el acceso a las comunicaciones privadas provenga de un serio debate legislativo; tome las precauciones del caso para no incurrir en violaciones al derecho a la intimidad al limitar, por ejemplo, en el tiempo la guarda de datos de tráfico; sea motivada y fundada; no posea vaguedades; se tomen medidas que razonablemente garanticen que los datos personales registrados no sean utilizados para fines distintos que los previstos en la norma.

Por tales motivos, el dato de las telecomunicaciones previsto por el Convenio de Budapest sólo podrá ser tratado en la medida que cumpla con los requisitos recientemente enumerados.

Aclarado ello y con relación al tratamiento de datos que el Convenio propone, cabe señalar que, al adjudicar poderes y procedimientos sólo a los efectos de "investigación o procedimientos penales específicos", cumple acabadamente con lo dispuesto en el art. 4, inc. 3 de la ley 25.326: "Los datos objeto de tratamiento no pueden ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención".

Asimismo, el Convenio dispone aplicar los poderes y procedimientos sometiéndose a las condiciones y garantías dispuestas en el derecho interno de cada estado, asegurando una protección adecuada de los derechos del hombre y de las libertades; incluyendo, cuando es posible, la supervisión judicial u otras formas de supervisión independiente, la motivación justificante de la aplicación, la limitación del ámbito de aplicación y la duración del poder o del procedimiento en cuestión. Obviamente, el respeto a los derechos del hombre como condición de aplicación del Convenio es una directriz en consonancia con nuestra Constitución Nacional.

Sin perjuicio de ello, merece especial consideración la frase que requiere el control judicial "cuando ello sea posible". Tal reserva podría permitir que, eventualmente, quede fuera del control judicial algún tratamiento de datos personales sobre el cual debiera aplicarse, por lo que hay que determinar dicho punto con mayor precisión, mediante mecanismos de reserva o declaración interpretativa del Derecho Internacional Público (Convención de Viena sobre Derecho de los Tratados).

El Convenio prevé empoderar a la autoridad competente para ordenar a una persona la conservación inmediata de datos electrónicos especifica-

dos que se encuentren bajo su poder y control —incluidos los datos de tráfico—, manteniéndolos íntegros, y durante el plazo que sea necesario hasta un máximo de 90 días, conservando el secreto de dichas medidas. Que los datos sean específicos —o sea, referidos a una solicitud concreta—, denota una restricción del dato a lo estrictamente necesario. Cumple con un criterio de calidad del dato del art. 4 de la ley 25.326, al que ya nos hemos referido. Por su parte, la exigencia de normas de seguridad y confidencialidad cumple con las disposiciones de los arts. 9 y 10 de la ley 25.326.

También empodera a la autoridad competente para ordenar a una persona la comunicación inmediata de datos electrónicos especificados que se encuentren bajo su poder y control —incluidos los prestadores de servicios—, almacenados en un sistema o soporte de almacenaje informático. La comunicación inmediata responde a la necesidad de la investigación y no representa en sí mismo un perjuicio para el titular; por lo que no afecta la calidad del dato en su tratamiento.

Otra de sus normas permite a la autoridad competente registrar o acceder a un sistema informático específico o soporte de almacenamiento informático específico y a los datos en ellos contenidos; decomisar u obtener de un modo similar dichos datos a los que haya tenido acceso; realizar y conservar una copia de los mismos y tomar las medidas necesarias para preservar la integridad de los datos informáticos pertinentes y exigir a la persona que conozca el funcionamiento del sistema informático o medidas aplicadas para su protección, que proporcione todas las informaciones razonablemente necesarias para aplicar las medidas correspondientes.

Al respecto, se entiende que la capacidad de la autoridad competente para registrar o acceder a un sistema informático es más que razonable para el ejercicio de sus facultades investigativas en un proceso penal. No obstante, en cuanto a la facultad de decomisar datos —dados los efectos negativos que eventualmente puede ocasionar dicha medida—, debería ser restringida a casos limitados y específicamente fundados en el expediente judicial.

Se prevé empoderar a la autoridad competente para recolectar o grabar, e interceptar datos de tráfico en tiempo real. Si el ordenamiento jurídico

interno de un estado no permite la grabación genérica de los datos de tráfico, debe preverse cuanto menos la grabación en tiempo real de datos de tráfico de comunicaciones específicas; manteniendo siempre el prestador de servicios el secreto de tales operaciones e información. La flexibilidad que entendemos que detenta el Convenio en este punto, al permitir la grabación de datos de tráfico sólo para comunicaciones específicas, o sea, para casos determinados, la califica como razonable; y como un tratamiento de datos pertinente, no excesivo; de acuerdo al principio de calidad de los datos ya referido.

En otro orden de ideas, los deberes de confidencialidad y seguridad de los datos personales exigidos por los arts. 9 y 10 de la ley 25.326, no están afectados por las previsiones del Convenio.

En igual sentido, las previsiones del Convenio no se oponen a los requisitos que la ley 25.326 establece respecto de la cesión de datos personales.

Así, el Convenio establece que la recolección de los datos mediante cesión de entes privados sea a través de los titulares de los bancos de datos o de los prestadores de servicios informáticos. Ésto condice con lo previsto en la ley 25.326, que expresamente exime de consentimiento del titular del dato cuando "se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal".

Asimismo, prevé la cesión de datos tanto al momento de su recolección como también en otras ocasiones. Por ejemplo, en los casos de cooperación internacional. La ley 25.326, expresamente exceptúa el consentimiento del titular del dato para los casos en que la cesión consista en una obligación legal.

Finalmente, y en cuanto a la transferencia internacional de datos regulada por el art. 12 de la ley 25.326; la norma dispone que no pueden cederse datos personales a países sin legislación adecuada. Con excepción expresa en los casos de colaboración judicial internacional; cuando la transferencia se acuerde en el marco de tratados internacionales en los cuales la República Argentina sea parte y cuando la transferencia tenga por objeto la cooperación internacional entre organismos de inteligencia para la lucha contra el crimen organizado, el terrorismo y el narcotráfico. Ello

implica que podrán cederse los datos previstos en el Convenio a países sin legislación adecuada, tomando resguardos para la debida protección de los datos personales a transferir.

6 | Conclusión

De acuerdo a los distintos aspectos que se han ido analizando, puede decirse que el Convenio de Budapest es, en líneas generales, compatible con las disposiciones de la ley 25.326.

Al momento de su aplicación, solamente deberá tenerse en cuenta que se tomen todos los recaudos que, conforme a nuestro derecho, resulten necesarios para una adecuada protección de los derechos de la persona., Pues debe tenerse presente que "en un régimen republicano la concreción de la necesidad pública estará dada justamente por el respeto estricto del interés privado de cada uno de los ciudadanos".[17]

(17) CNac. Cont. Adm. Fed., sala II "Halabi Ernesto c/ PEN Ley 25.873 - decreto 1563/04 s/ amparo ley 16.986", 29/11/ 2005.

Protección penal de la privacidad en la "sociedad de la información"

Análisis de la ley 26.388 y algunas consideraciones preliminares en torno al Anteproyecto de Código Penal de la Nación

por **HORACIO SANTIAGO NAGER**[1]

1 | Introducción

El presente trabajo tiene por objeto analizar el impacto que han significado las nuevas tecnologías de la información en un bien jurídico fundamental: la intimidad o privacidad de las personas, y en pos de cumplir con el objetivo trazado, nos centraremos especialmente en las figuras legales modificadas y/o introducidas por la Ley de Delitos Informáticos 26.388.

Asimismo, dedicaremos algunos breves párrafos a conductas, cuya tipificación fue discutida en los recintos legislativos, pero que finalmente no merecieron recepción positiva.

(1) Especialista en Derecho Penal (UBA). Auxiliar docente del Departamento de Derecho Penal y Criminología de la Facultad de Derecho (UBA), en la asignatura Elementos de Derecho Penal y Procesal Penal, cátedra del Prof. Alejandro Alagia. Prosecretario Letrado de la Defensoría General de la Nación.

Finalmente, procuraremos realizar un breve análisis sobre las reformas que el reciente Anteproyecto de Código Penal de la Nación propone en la temática.

2 | Bien jurídico protegido

A raíz de la sanción de la Ley de Delitos Informáticos (ley 26.388) modificó el epígrafe del Capítulo III, del Título V del Código Penal, definiendo el legislador los contornos materiales del bien jurídico tutelado por las figuras penales allí previstas.

Tradicionalmente, la doctrina jurídico penal criticó la formulación del texto derogado, pues parecía circunscribir la protección legal a información y/o documentos cuyo contenido resultara secreto; sin embargo, esta impresión inicial, se revelaba errónea al reparar en las conductas allí tipificadas, ya que en aquel elenco penal se punían acciones lesivas de la intimidad de las personas. De esta forma, se ha corregido un error histórico, porque la correspondencia y los papeles privados no constituyen necesariamente cosas secretas.(2)

Ahora bien, con respecto al término escogido en la ley 26.388, cabe advertir que lo privado puede no ser lo íntimo, de manera que el legislador optó por la fórmula más amplia a la hora de receptar posibles actos lesivos al núcleo ético social protegido. Esta elección terminológica se encuentra muy posiblemente inspirada en el derecho anglosajón donde, desde antiguo, se ha definido a la privacidad como el derecho a estar libre de injerencias indebidas o arbitrarias, sea que éstas provengan de terceros o del Estado. Por cierto, en el *common law* norteamericano esta garantía material, bajo el rótulo de *right of privacy,* ha sido definida como el derecho que cada individuo tiene a permanecer aislado, solo, dentro de una esfera de reserva o exclusión de la injerencia de otros individuos o del Estado; o sea, "como el derecho de vivir sin interferencias no deseadas por el público, sobre asuntos que no están necesariamente relacionados con éste".(3)

(2) Molinario, Alfredo J., *Los Delitos*, (preparado y actualizado por Eduardo Aguirre Obarrio) Bs. As., TEA, 1996, t. II, p. 108.

(3) *Enciclopedia Jurídica Omeba* (versión digital), voz "*intimidad (derecho a la)*", tema desarrollado por el Dr. Mateo Goudstein.

Sin perjuicio de ello, a los fines de este trabajo, y en lo que respecta al tratamiento dogmático de los delitos que integran este capítulo, usaremos en forma indistinta los términos "intimidad" y "privacidad".

No está demás puntualizar, siguiendo a Moeremans que:

> "... sobre la intimidad se han pronunciado infinidad de definiciones y teorías. Pero al ser éste un elemento vivo, que responde a las circunstancias, que debe adaptarse a cada momento y tiempo social, sus manifestaciones se encuentran debatidas. Siguiendo la teoría de las Esferas podemos distinguir en: La esfera íntima: es lo intangible de la persona, sus atributos, pensamientos, que de modo alguno influyen en la sociedad. La esfera privada: se compone por las ideas compartidas con familiares, amigos, por las acciones que se realizan sin menoscabo de derechos de terceros. La esfera social: son las acciones que entran en la interacción social…".(4)

Una breve referencia histórica sobre el bien jurídico, en tanto constituye una de las manifestaciones de la libertad humana, resultará ilustrativa al objeto de comprender el enorme desafío que plantea la sociedad ultra tecnificada del siglo XXI.

La libertad de intimidad es un derecho de base ilustrada que surgió en los albores del Estado Moderno como una reacción contra el sistema monárquico y absolutista del Antiguo Régimen, cuya piedra fundacional reside en el reconocimiento del principio de dignidad y autodeterminación ética de la persona humana. En dicho marco histórico, el acceso al conocimiento por parte del ciudadano encontró directa vinculación con los valores revolucionarios de libertad e igualdad, que se erigió en una pieza fundamental para el avance del humanismo y la ciencia, en contraposición con el oscurantismo medieval. Sin dudas, los cambios fueron progresivos, y la evolución jurídica no fue siempre acompañada por la consecución concreta de estos derechos, devenidos también en garantías.

(4) Moeremans, Daniel E., "Protección del e-mail como extensión del derecho a la intimidad", en *Revista Jurídica La Ley*, 2007-E, p. 740.

Sin embargo, resulta innegable que el derecho a la privacidad constituye un límite racional y concreto al poder público y a terceros. Los Estados autoritarios tienden a difuminar sus límites permitiendo injerencias arbitrarias en la esfera de reserva de las personas, mientras que el Estado de derecho tiene la obligación de proteger este espacio donde el individuo tiene "derecho a estar solo", como una de las manifestaciones más importantes de la libertad personal.

Ya inmersos en el siglo XX, la protección de la intimidad se intensificó al finalizar la segunda guerra mundial, a raíz de la preocupación de la comunidad internacional por las prácticas de espionaje, tal como quedara expuesto en la Declaración Universal de Derechos del Humanos (art. 12).[5]

Como hemos visto, en el pasado el monopolio de la información y la censura implicaba la principal manifestación de poder; actualmente dicho poder no reside solamente en el acceso o la supresión de los datos,[6] sino también en las posibilidades que ofrece su tratamiento, y en la capacidad de discernir entre la información confiable de aquella que no posee tales características. Por otro lado, las conductas susceptibles de afectar este bien jurídico se han incrementado sensiblemente en términos de intensidad e inmediatez de la mano del fenómeno de la globalización.

Por último, debemos recordar que la intimidad constituye un derecho personalísimo, y como tal, es inherente al ser humano por su sola condición de tal.

3 | Los desafíos que plantea la protección de la privacidad en la "sociedad de la información"

En relación con lo expuesto anteriormente, resulta innegable que en las últimas décadas, y de manera cada vez más acelerada, se han producido

(5) Adoptada y proclamada por la Asamblea General en su Resolución 217 A (III), del 10/12/1948.

(6) Sobre el acceso igualitario y libre a la información almacenada en Internet se recomienda ver Tomeo, Fernando, "La neutralidad en Internet", en *Revista Jurídica La Ley*, 2011-E, 1367.

importantes avances tecnológicos en materia de comunicaciones; lo que constituye uno de los datos sociológicos por excelencia de este siglo, a punto tal que frecuentemente, escuchamos decir que vivimos en la "sociedad de la información".

Como manifestación negativa del incesante desarrollo de estas herramientas técnicas, se advierte que el ámbito de reserva o privacidad del individuo nunca ha sido tan vulnerable, y que se ha quebrado, al menos en parte, aquel vínculo ilustrado entre libertad de acceso a la información y libertad individual. En este sentido, basta detenerse unos instantes en la conexión que existe (al menos en el plano discusivo) entre la "sociedad de la información" y la "sociedad del riesgo", con sus súbitas y controvertidas emergencias.(7) Todo lo cual, repercute a la hora de recortar progresivamente el ámbito de reserva personal, permitiendo una mayor injerencia del Estado en la vida privada.

(7) Por ejemplo, la invocación de la lucha contra el terrorismo internacional y guerra preventiva como fundamento de la existencia de sistemas de espionaje global como *Carnivore* (FBI) y *Echelon* (NSA). El primero de estos sistemas de vigilancia a distancia de origen estatal es "… un software usado por el FBI que (…) se instala en los proveedores de acceso a Internet y, tras una petición proveniente de una instancia judicial, rastrea todo lo que un usuario hace durante su conexión a Internet (Ver [en línea] http://www.wikipedia.org). Sus críticos "… advierten que su poder es ilimitado (…) tiene la capacidad de filtrar en busca de determinadas palabras clave millones de mensajes de correo electrónico que viajan por la Red y sin saber que son vigilados. El programa tiene unas claves, que el FBI mantiene en secreto, que permiten descubrir la información que la agencia policial busca. Estas claves pueden ser palabras, nombres de políticos, de ciudades, y terminología que levante sospechas entre los investigadores del FBI. Cuando uno de estos mensajes es localizado, el programa se introduce en el disco duro del internauta 'capturado' y archiva toda su información confidencial, a la espera de que los investigadores determinen si ha cometido algún delito. Incluso antes de un juez les dé permiso para hacerlo."; no obstante, en el año 2005, el gobierno estadounidense, anunció el cese del uso de este programa especial de vigilancia por Internet, al tiempo que requirió a los servidores de servicios de Internet que vigilen a sus clientes (ver [en línea] http://www.elmundo.es). Por su parte, Echelon "... es considerada la mayor red de espionaje y análisis para interceptar comunicaciones electrónicas de la historia. Controlada por la comunidad UKUSA (Estados Unidos, Reino Unido, Canadá, Australia, y Nueva Zelanda) (…) puede capturar comunicaciones por radio y satélite, llamadas de teléfono, faxes y e-mails en casi todo el mundo e incluye análisis automático y clasificación de las interceptaciones. Se estima que Echelon intercepta más de tres mil millones de comunicaciones cada día". (ver [en línea] http://www.wikipedia.org). Precisamente, este poder de control y espionaje masivo ha sido desde el año 2009 el eje de un escándalo internacional generado a partir de la revelación de documentos clasificados pertenecientes al gobierno de los EEUU, gracias al incidente conocido como "WikiLeaks" y el aporte posterior del ex analista de la CIA Edward Snowden. Escándalo que culminó en la modificación de la ley de inteligencia de ese país del Norte.

Precisamente, una de las notas características de las sociedades postmodernas es el aumento de los riesgos humanos de la mano de la evolución tecnológica, como un efecto colateral de las grandes ventajas que este desarrollo provee a la vida social. Por ello, el nexo que une a conceptualizaciones sociológicas como la "sociedad de la información" y la "sociedad del riesgo" es el auge técnico (muchas veces de origen militar) que se ha incrementado exponencial e incesantemente desde la invención de la máquina de vapor. Criminológicamente, este binomio también se complementa y retroalimenta, pues la sociedad del riesgo requiere nuevas técnicas de control social, dentro de las cuales, el monitoreo de personas, el control y tratamiento del tráfico de datos privados, el "espionaje" y otras tecnologías son presentadas como herramientas eficaces y útiles, que posibilitan nuevos mecanismos de control justificados en criterios utilitaristas y modelos de gestión de riesgos que bien podrían significar una vuelta del viejo peligrosismo. Así, diversos ensayistas refieren que vivimos bajo una **libertad vigilada** o en una **casa de cristal**; mientras otros, señalan una contraposición dialéctica entre dos modelos bien diferenciados: por un lado, la concentración y control de la información en manos de unos pocos ("*Big Brother*"), y por el otro, el acceso irrestricto a la información como una suerte oráculo al alcance de todos. A esta altura, la mención de las distopías del siglo XX de Aldous Huxley[8] y Eric Blair —mejor conocido como George Orwell—[9] resulta inevitable.

En sintonía con lo anterior, Zygmunt Bauman entiende que vivimos en los tiempos del modelo post-panóptico, sujetos al control de vigilantes que ya no tienen la necesidad de atarse al espacio para cumplir con su tarea, ni de encerrar al sujeto a observar en instituciones totales. En otras palabras, el control (electrónico) se ejerce en tiempo real y a distancia, con un grado de eficiencia aún mayor. No olvidemos que por diversas razones (por ejemplo, seguridad pública, control del tránsito, cuidado de plazas, etcétera) nuestros movimientos quedan registrados, día a día, en sistemas de cámara de video instalados en espacios públicos.[10] Este fenómeno debe ser advertido, aunque resulta obvio que la tecnología no es más que

(8) Huxley, Aldous, *Un mundo feliz*, Bs. As., Sudamericana, 1958.

(9) Orwell, George, *1984*, Madrid, Salvat, Editores S. A., 1971.

(10) Merece mencionase la resolución 415/2004 del Ministerio de Justicia, Seguridad y Derechos Humanos, en virtud de la cual se creó el registro de huellas digitales genéticas, en el ámbito de la Policía Federal Argentina, la existencia de sitios de Internet como "23andMe", etcétera.

una herramienta, en sí misma "neutral"; por lo que corresponde centrar el debate en la forma y los fines con que se la emplee en el caso concreto.

No podemos dejar de mencionar en estos párrafos introductorios, la proliferación de herramientas de uso civil como "Google" y sus distintas aplicaciones,[11] *Facebook*[12] *You Tube, Fotolog, Twitter,* etcétera, en las cuales se perciben importantes cambios culturales en torno a la distinción entre lo público y lo privado, con fuerte impacto en el sustrato material del bien jurídico en trato. Esta cuestión, sin perjuicio de que su debido abordaje corresponde a la sociología, deviene palpable, y en esa dirección se ha dicho, por ejemplo, que:

> "... la intimidad se mira como un valor retrógrado, represivo, puritano (…) De ahí el auge, a veces desmedido de los *reality shows*, donde la vida transcurre en vivo y a la vista de audiencias multitudinarias; de facebooks y sitios similares donde cada uno muestra sus fotos, sus preferencias, sus conversaciones, sus amigos, su humor, sus datos de contacto; de blogs que lo cuentan todo. No hay filtros, o siquiera los menos posibles, para no traicionar el ideal de total transparencia…"[13]

Asimismo, se sostiene que *Twitters, Facebooks* y demás "bellezas informáticas" han logrado meterse en la vida privada de todos los que, muchas veces involuntariamente y sin ningún tipo de aviso previo, son sometidos a vejámenes, indiscreciones y bochornos y que:

> "… de nada se vale que uno se resguarde evitando pertenecer a red social alguna. Nada importa. Puede haber 'otros yo' que con tu nombre digan lo que les dé la gana y hablen por uno dando opiniones que nada tienen que ver con nuestra ideología

(11) Sobre este tema se recomienda la lectura del siguiente trabajo: Palazzi, Pablo A., "Google y el Derecho a la Privacidad sobre las búsquedas realizadas en Internet", *RCE* n° 74, 2006, pp. 31/40.

(12) Se ha destacado que "Lo extraordinario de Facebook respecto de Google es que no hacen falta algoritmos para conocer las preferencias del público. Las personas ceden esta información por voluntad propia". Ver Torres, Ariel, "¿Es Facebook el próximo Google?", en diario *La Nación*, Bs. As., edición impresa 09/01/2011, p. 2.

(13) Batallanez, Teresa,"La intimidad al desnudo", en revista *La Nación*, Bs. As., 09/01/2011, p. 74.

> de vida (…) Casi todas las constituciones democráticas, incluida la argentina, resguardan el derecho a la intimidad, y en casi todas las sociedades es negada, burlada y ofendida (…) hoy en día no sólo se trata del espionaje político para detectar enemigos opositores, sino de pura y dura violación del sagrado derecho a ser quien uno quiera ser sin la obligación de compartirlo con desconocidos".(14)

Al mismo tiempo, resulta paradojal que la mayoría de los usuarios de Internet no confíen en la seguridad de la red, más no adopten recaudo alguno a fin de utilizarla de modo seguro —por ejemplo: *firewalls*, claves seguras, cifrado y borrado seguro de datos, antivirus y anti-*spywares* actualizados, navegación anónima, etcétera—. En este punto, lejos de propiciar la incursión en políticas paternalistas o perfeccionistas, creemos que los Estados debieran incluir programas públicos destinados a fomentar el uso responsable e informado de estas nuevas tecnologías, lo que entendemos hallaría asidero y armonía con el carácter de *ultima ratio* del sistema penal. De lo contrario, antes de implementar medidas de prevención, seguramente más idóneas, seguiremos recurriendo al derecho penal en su función preponderantemente simbólica, si tenemos en cuenta el alto porcentaje —"cifra negra"—, que caracteriza a estos delitos y las dificultades que éstos presentan de cara al dictado de una eventual sentencia de condena.(15)

De esta manera, para dotar de racionalidad y proporcionalidad a la potestad punitiva del Estado no debería perderse de vista cuáles son los contornos actuales del bien jurídico "privacidad" a la luz de las nuevas prácticas y costumbres sociales, deteniéndonos unos instantes, en el rol de la víctima, en función de su "autopuesta" en peligro —consciente o no— como elemento de recorte de la tipicidad objetiva o, en su defecto, como pauta mensurativa de la pena. Con esto, no buscamos relativizar la trascendencia del bien jurídico sino evitar una aplicación de las normas mecánica y ajena de la realidad, que se base en una visión idealizada de

(14) Pinti, Enrique, "*1984 es el pasado*", en revista *La Nación*, 26/12/2010, p. 18.

(15) Así se ha informado que: "... las encuestas indican que cada cuatro delitos informáticos, sólo uno es denunciado. La conducta que con mayor frecuencia se reporta es el robo de contraseñas o claves de acceso. En los tribunales de la Capital Federal ya se registraron 8425 denuncias por "ciberdelitos" durante los últimos cuatro años y medio" (fuente: Profesional.com del 28/06/2010).

la sociedad que sólo persiga una finalidad preventivo general, en su faz positiva. En otras palabras, la conducta del usuario es imprescindible en la búsqueda de la seguridad informática, y por lo tanto, el Estado debe asumir la obligación de concientizar a la población acerca de los riesgos que conlleva el uso desaprensivo de estas herramientas tecnológicas, pues sólo así cada individuo será realmente libre a la hora de ejercer su derecho a la privacidad en el espacio virtual.

Asimismo, cabe apuntar que en este mundo globalizado las desigualdades sociales se manifiestan también en torno al acceso y manejo de estos nuevos instrumentos, verificándose una ostensible "brecha digital",(16) dentro de las fronteras de un país, e incluso entre los diferentes Estados Nación; circunstancia que no sólo parece otorgar razón a quienes endilgan al proceso de mundialización —fuertemente favorecido por las nuevas tecnologías de la información— un carácter unidireccional, sino que también plantea serias dificultades a los sistemas de administración de justicia locales, si se tiene en cuenta que el ciberespacio no se ve limitado por reglamentaciones de derecho interno. Sobre este tópico, en los debates parlamentarios se dijo que debía brindarse:

> "... la mayor libertad posible en el uso de los ordenadores, de la red y de las comunicaciones, porque es la única forma en que se podrá aumentar la posibilidad de que el usuario —en el caso de la Internet— se apropie de una tecnología que no sea de dominio exclusivo de grupos o países (…) Después de la escritura y de la imprenta aparece lo que hoy se denomina la hipermedia, el hipertexto, la red o el ordenador. Al igual que la escritura y la imprenta va a modificar no solamente las formas del desarrollo que el ser humano tiene en cuanto a la comunicación, sino que también modificará la relaciones de producción (…) la tecnología no es buena ni mala, ni neutral, está ahí, construye las sociedades y la cultura, se mete en la dinámica social y modifica las relaciones sociales".(17)

(16) Ver al respecto, el contenido de la *Declaración del Milenio* aprobada por la Asamblea General de las Naciones Unidas, [en línea] http://www.un.org/spanish/milenio/ares552.pdf.

(17) Nemirovsci, Osvaldo M., Cámara de Diputados de la Nación, Secretaria Parlamentaria, Dirección de Información Parlamentaria, 34ª Reunión - 25ª Sesión Ordinaria, 11/10/2006 (versión taquigráfica).

En razón de lo expuesto, las posibilidades que brinda la tecnología para vulnerar el bien jurídico privacidad conlleva serios riesgos para la vigencia real del Estado de derecho, correspondiendo a sus distintas agencias —especialmente, las ejecutivas— no sólo abstenerse de espiar indebidamente a los individuos, sino también asumir la obligación y el desafío de idear e implementar políticas públicas que resguarden esta manifestación de la libertad individual. La vigencia práctica de los derechos constitucionales y las garantías del justiciable reclama más que nunca el respeto de los límites formales y materiales que racionalizan y humanizan el ejercicio de la potestad punitiva. En esta convicción, rechazamos los intentos de flexibilización de garantías procesales y sustantivas a través de la aceptación de un nuevo estándar procesal que ha recibido en la doctrina la denominación de "Derecho Procesal Penal del Enemigo",[18] que bajo el argumento de combatir nuevas y más peligrosas formas de delincuencia transnacional, se propone reformular o "modernizar" las bases del derecho penal liberal.

Por último, y sin perjuicio de exceder el objeto de este trabajo en función del bien jurídico que nos ocupa, baste mencionar que la informática en general, representa riesgos para los Estados Nación, y tanto más, a medida que avanza la automatización de servicios públicos o el denominado *e-goverment*.

4 | Marco normativo convencional, constitucional y legal

La **privacidad** halla recepción positiva en diversos instrumentos normativos de naturaleza convencional, constitucional y legal. Así, nuestra Carta Magna en sus arts. 18 y 19 establece que "el domicilio es inviolable, como también la correspondencia epistolar y los papeles privados; y una ley determinará en qué casos y con qué justificativos podrá procederse a su allanamiento y ocupación" y que "las acciones privadas de los hombres que de ningún modo ofendan al orden y a la moral pública, ni perjudiquen a un tercero, están sólo reservadas a Dios, y exentas de la autoridad de los

(18) Sobre este tema, ver Muñoz Conde, Francisco, "De las prohibiciones probatorias al Derecho procesal penal del enemigo", *Claves del Derecho Penal*, Bs. As., Hammurabi, 2008..

magistrados". Por otro lado, la reforma constitucional de 1994 influyó en la protección jurídica de este derecho/garantía, en su faz de libertad de autodeterminación informativa, ya que estableció en el art. 43 que toda persona podrá interponer acción de amparo "… para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquéllos. No podrá afectarse el secreto de las fuentes de información periodística". A su vez, mediante la cláusula contenida en el art. 75, inc. 22 CN incorporó con jerarquía constitucional los tratados internacionales de Derechos Humanos, destacándose en lo que a la libertad de intimidad o privacidad se refiere, el art. 11 (incs. 2 y 3) de la Convención Americana de Derechos Humanos, el art. 17 del Pacto Internacional de Derechos Civiles y Políticos, el art. 12 de la Declaración Universal de Derechos Humanos, y el art. 11 de la Declaración Americana de Derechos y Deberes del Hombre.

No puede pasarse por alto la opinión de un sector de la doctrina, en cuanto se refiere a la irrupción de un nuevo bien jurídico: "la protección de los datos personales". De esta manera, en relación a los tipos penales previstos en los arts. 117 *bis* y 157 *bis* del Código Penal, se ha dicho que:

> "… no protegen los bienes jurídicos tradicionales como la fe pública, la confidencialidad o la privacidad, sino uno nuevo que es la protección de los datos personales (…) La incolumidad de la información almacenada en bases de datos debe preservarse porque sobre esos datos se toman decisiones y ellas pueden perjudicar y afectar a individuos y titulares de datos personales".(19)

Creemos que el reconocimiento de este nuevo bien jurídico, distinto de aquél previsto en el epígrafe del Capítulo III, Título V, Libro II del Código Penal, si bien posee atendibles fundamentos, resulta opinable desde la perspectiva que imponen los principios jurídicos reductores del ámbito de intervención del derecho penal, pues se corre el riesgo de ampliar la potestad punitiva en desmedro del justiciable; máxime, cuando estamos

(19) Palazzi, Pablo A., *Los Delitos Informáticos en el Código Penal. Análisis de la ley 26.388*, Bs. As., Abeledo-Perrot, 2009, p.142.

ante delitos de acción privada, pues la tesitura antedicha podría incidir en adjudicar legitimación procesal para querellar, a quien de otra manera, carecería de tal derecho. Además, sin soslayar la existencia de nuevos derechos y garantías, téngase presente que durante la Convención Constituyente, al analizar el texto del art. 43 CN, se dijo que:

> "... el tercer párrafo alude a un ámbito de derechos personales en el marco de una realidad donde la acumulación de información y su manipulación han generado amenazas y daños tremendos a las personas y a sus derechos. Estamos en presencia de una acción destinada a proteger el derecho a la privacidad, a la intimidad, derecho contemplado en el art. 19 de la CN. Con ello se incorpora una protección efectiva ante el avance de un fenómeno nuevo y poderoso que puede exceder el ámbito de las garantías y defensas clásicas (…) Esta incorporación (…) es por demás relevante, máxime considerando las aciagas épocas del autoritarismo, en donde la inclusión de datos de personas en determinados registros podía implicar desde la incorporación en las llamadas "listas negras" con discriminaciones y atropellos consiguientes, hasta la pérdida de la libertad o la vida".[(20)]

En esta inteligencia, en la hermenéutica de la norma penal, el bien jurídico es la privacidad, y la protección de datos personales es una manifestación del primero, y no constituye un concepto jurídico autónomo, encontrando un claro referente o sustrato material en dicho atributo de la personalidad.

A nivel interno, el derecho a la privacidad se encuentra contenido en las constituciones locales,[(21)] como también en los códigos sustantivos, diversas leyes especiales y los digestos de forma. Así, a título meramente ilustrativo, podemos mencionar los arts. 1071 CC; 153 a 157 *bis* CP; 235 y 236 CPPN y las leyes 24.766, 25.326, 25.520 y 25.873; etcétera.

(20) Debate del dictamen de la Comisión de Redacción en los despachos en mayoría y minoría originados en la Comisión de Nuevos Derechos y Garantías (Orden del Día Nº 11), Sesión 3ª, reunión 31ª, 16/08/1994, p. 4284, Solicitada de la Sra. Convencional Arellano, [en línea] http://www.infoleg.gov.ar.

(21) Ver arts. 12 inc. 3, 13 inc. 8 y 16 de la Constitución de la CABA; arts. 12 incs. 3, 4, 5 y 20 inc. 3 de la Constitución de la provincia de Buenos Aires, etc.

5 | Análisis dogmáticos de los tipos penales previstos en la ley 26.388

5.1 | Artículo 153 del Código Penal

La sanción de la ley 26.388 obedeció a la necesidad de actualizar la legislación penal a las demandas de la "sociedad de la información", en la que a la par de observarse el decrecimiento del uso del correo epistolar, se produjo la irrupción de nuevas formas de comunicación, tales como el *e-mail,* el *chat* (palabra del idioma inglés que significa "charla" o "charlar"), las redes sociales, el SMS *(Short Message Service)*, etcétera.

En este sentido, resultan ilustrativas las palabras del diputado Nemirovsci:

> "Obviamente, al redactar el Código Penal el legislador no podía prever en 1921 —tampoco en ninguna de las 800 modificaciones que se han introducido desde entonces— la comisión de delitos a través de la informática y de las nuevas tecnologías. Por eso hoy le damos la bienvenida a toda iniciativa que venga a llenar ese vacío legal (…) no estamos sancionando una ley de delitos informáticos que crea nuevas figuras penales. Simplemente estamos adaptando los tipos penales a las nuevas modalidades delictivas".[22]

A su vez, el proceso legislativo —iniciado en el año 1996 con el proyecto de Leonor E. Tolomeo— se aceleró al hacerse público en el año 2006 un caso de intrusismo informático sobre correos electrónicos pertenecientes a políticos, jueces y periodistas, de reconocida trayectoria.[23]

(22) Cámara de Diputados de la Nación, Secretaria Parlamentaria, Dirección de Información Parlamentaria, 34ª Reunión – 25ª Sesión Ordinaria, 11/10/2006 (versión taquigráfica).

(23) A fin de conocer los antecedentes históricos de la Ley 26.388, publicada en el BO el 25/06/2008, puede consultarse el siguiente trabajo: Fillia, Leonardo C.; Monteleone, Romina *et al.*, "*Análisis a la reforma en materia de criminalidad informática al Código Penal de la Nación*", *La Ley* Suplemento Penal, agosto 2008, p. 15. Asimismo, en relación a los hechos de público conocimiento que aceleraron el *iter* legislativo, resulta pertinente citar las siguientes expresiones de la diputada Norma Elena Morandini: "Se moderniza el espionaje, que ahora es electrónico, pero no se erradica la vieja práctica del chantaje. Los datos jaqueados, como demostró la denuncia que inspiró los proyectos en que se basa el dictamen de comisión,

Este episodio colocó nuevamente en la escena pública la discusión sobre la interpretación del derogado art. 153 del Código Penal a la luz del principio de legalidad. Antes de la sanción de la ley 26.388, un sector de la doctrina proponía una interpretación extensiva, teleológica, progresiva o dinámica de las leyes por imperio histórico. Así, por ejemplo, el constitucionalista Gregorio Badeni opinaba que "frente a tales adelantos es necesaria una razonable interpretación dinámica de las leyes para que, sin necesidad de acudir a su reforma, se pueda evitar que queden a la zaga de la realidad social" y Creus —en sintonía— afirmaba que "salvo casos de conceptualizaciones terminantemente limitativas de su sentido, acompañar las transformaciones técnicas ampliando, para comprenderlas, el significado de las acciones típicas respecto del que poseían en tiempos pretéritos de la evolución técnica no es hacer analogía sino interpretar".(24) Otro segmento de la academia, rechazaba esta exégesis de la ley, acusándola de constituir una forma solapada de extensión analógica del tipo penal, vedada al intérprete por imperio del principio de legalidad, en su función de *lex stricta*. La jurisprudencia no era uniforme sobre el tópico, se establecieron, como habitualmente sucede, dos posturas. La Sala VI de la Cámara Nacional en lo Criminal y Correccional —integrada por los Dres. Ameghino Escobar, Elbert y González—, en el caso "Lanata, Jorge s/ desestimación", de fecha 04/03/1999, sostuvo que :

> "Nada se opone para definir al medio de comunicación electrónico como un verdadero correo en versión actualizada. En tal sentido la correspondencia y todo lo que por su conducto

se utilizaron para controlar los movimientos de un periodista, un funcionario o un juez, para mapear sus relaciones y hacerles sentir (insisto con esta idea) que están siendo controlados. De alguna manera todos tenemos naturalizado que algunas cuestiones no se pueden hablar por teléfono…". (Ver Cámara de Diputados de la Nación, Secretaria Parlamentaria, Dirección de Información Parlamentaria, 34ª Reunión - 25ª Sesión Ordinaria, 11/10/2006 (versión taquigráfica).

(24) Creus, Carlos, "El miedo a la analogía y la creación de vacíos de punibilidad en la legislación penal (intercepción de comunicaciones telefónicas y apropiaciones de e-mail)", *JA*, 1999-IV-869. Este autor, pese a estar a favor de la interpretación dinámica de la ley penal, sostenía que considerar como objeto del delito de violación de correspondencia al correo electrónico era hacer analogía, ya que sus textos podían ser leídos en la pantalla tal como le han sido remitidos al destinatario. Nada se "abre", pues nada está cerrado. Sin embargo, opinaba que eso no sucedía, si se consideraba objeto material de los delitos previstos en el art. 153 (segunda figura) y 155 del Código Penal al correo electrónico, ya que en estos casos la acción típica no es la de "abrir" sino la de "apoderarse" y "publicar respectivamente".

> pueda ser transmitido o receptado, goza de la misma protección que quiso darle el legislador al incluir los arts. 153 a 155 del CP, en la época de su redacción, cuando aún no existían estos avances tecnológicos".

Sin embargo, algunos tribunales adoptaron la postura contraria, como el Juzgado Nacional en lo Correccional N° 9, que en la causa "Gálvez, Esteban", del 11/04/2007, rechazó la asimilación del correo electrónico a la correspondencia privada, señalando que:

> "... el principio de máxima taxatividad legal e interpretativa se manifiesta mediante la prohibición absoluta de la analogía 'in malam partem', lo que se verificaría si en la especie se intentara forzar la interpretación que inveteradamente se ha dado no sólo en lo concerniente al objeto de protección de la norma del art. 153 del código sustantivo, sino a sus quehaceres típicos, por lo que resulta inaceptable dar cabida a la presente querella desde la norma escogida por la querella como la infringida por los intrusos, que accedieron a su correo del servidor Yahoo de Argentina SRL".

Esta discusión se encuentra zanjada a partir a partir de la entrada en vigencia de la ley 26.388, cuyo texto reza lo siguiente en su art. 4:

> "Será reprimido con prisión de quince días a seis meses el que abriere o accediere indebidamente a una comunicación electrónica, una carta, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, que no le esté dirigido; o se apoderare indebidamente de una comunicación electrónica, una carta, un pliego, un despacho u otro papel privado, aunque no esté cerrado; o indebidamente suprimiere o desviare de su destino una correspondencia o una comunicación electrónica que no le esté dirigida".

En primer término, es necesario advertir que el correo electrónico es un medio de comunicación inseguro que circula por la red a través de millones de nódulos y *routers*, pudiendo ser captado en cualquiera de estas fases. A su vez, el 50% del tráfico mundial de Internet pasa siempre por

el Estado de Virginia, EEUU, tal como lo revela Bárbara Cassin.[25] Como hemos anticipado, estas comunicaciones electrónicas pueden ser objeto de accesos ilegítimos o legítimos. No olvidemos que los ISP y los motores de búsqueda pueden registrar los datos de tráfico en servidores, o que empresas tales como *Hotmail, Gmail o Yahoo* —generalmente a través de rutinas automatizadas— pueden filtrar nuestras comunicaciones electrónicas a fin de optimizar el servicio (por ejemplo: eliminación o bloqueo de amenazas lógico informáticas, desvío de correo no deseado, etcétera). Así, es claro que más allá de que una finalidad legítima en su origen pueda mutar su naturaleza (transformándose en ilegítima), estas herramientas de comunicación moderna presentan no pocas vulnerabilidades desde el punto de vista técnico.

Núñez, definió a la correspondencia como "la comunicación por carta, pliego o despacho telegráfico, fonográfico o de otra naturaleza, enviada por un remitente a un destinatario", en la que se establece un diálogo.[26] Por papeles privados se entiende cualquier expresión de ideas escrita comprendida dentro del ámbito de reserva de una persona, y a su vez, a partir de la redacción típica del delito de "apoderamiento indebido de correspondencia u otro papel privado" parece englobarse dentro del género "papeles privados" a cartas, pliegos y despachos. Antes de la reforma, se decía que resultaba esencial que el papel escrito "se encuentre dispuesto en forma tal que no baste su simple desdoblamiento para que el texto se ofrezca a la vista" y que su contenido revista el carácter de íntimo o personal, no siendo aptas para configurar el tipo, por ejemplo, una simple nota o publicidad comercial.[27]

La ley 26.388 incluyó dentro del concepto amplio de **correspondencia** las comunicaciones electrónicas, apelando a un término susceptible de adaptarse, sin necesidad de una nueva reforma legal, a las incesantes innovaciones que deparan los avances tecnológicos a estas formas de

(25) Cassin, Bárbara, *Googléame. La segunda misión de los Estados Unidos*, trad. de Víctor Goldstein, Bs.As., Fondo de Cultura Económica, 2008, p. 25.

(26) Nuñez, Ricardo C., *Manual de Derecho Penal. Parte especial*, 2° ed. actualizada por Víctor F. Reinaldi, Córdoba, Marcos Lerner, 1999, p. 175.

(27) Ossorio y Florit, Manuel, *Código Penal de la República Argentina. Comentarios. Jurisprudencia. Doctrina. Legislación complementaria*, Bs. As., Universidad, 1979, p. 237.

comunicación.[28] Si bien la opción del codificador resulta adecuada, será tarea de la jurisprudencia delinear los precisos alcances de este elemento del tipo penal recurriendo a la función reductora del bien jurídico y a los mandatos del principio de legalidad. Por ello, y a título meramente enunciativo, pensamos que la inclusión legal no modifica las exigencias tradicionales de que la comunicación electrónica se encuentre dirigida a una persona —incluso podría tratarse del propio remitente que se envía un mensaje a sí mismo, por ejemplo, a modo de borrador o para acceder desde cualquier lugar al documento, si atendemos al concepto detrás del género papeles privados— y que su contenido revista carácter privado, no siendo accesible a simple vista. Esta aclaración viene al caso, pues en la Red existen numerosas operaciones automatizadas, donde difícilmente pueda afirmarse que se ha procurado entablar un diálogo con un interlocutor frente a la ausencia de un componente volitivo en dicho proceso comunicacional. Por su supuesto, la cuestión es compleja, pues estas funciones siempre son precedidas de una tarea de programación, por lo que a los fines de evitar una ampliación ilegítima del tipo penal, deberá establecerse en primer lugar a la naturaleza del contenido de la comunicación electrónica. Al respeco, Palazzi se pregunta si debe haber al menos un emisor o destinatario humano, respondiendo que de entenderlo así quedaran fuera de protección penal numerosas situaciones, ya que "hoy en día la relación con numerosas empresas y sistemas está automatizada a través de ordenadores, y con ellos también hay comunicación".[29] No estamos de acuerdo con este razonamiento porque la interpretación histórica del art. 153 del CP, el significado del término "comunicación"[30] y la naturaleza del bien jurídico, creemos que exigen, al menos, que interactúe un ser humano en alguna de las fases del proceso: emisor - mensaje - destinatario.

(28) Nótese que en una reciente nota titulada "El correo electrónico le deja su lugar a las redes sociales y al chat", se advierte que el uso extensivo de los mensajes de texto y las recientes modificaciones que realizó Facebook en su servicio de mensajería replantean el uso del e-mail en determinados entornos. Así se ha dicho, por ejemplo, que "el futuro de los mensajes es más en tiempo real, más dialogado y más informal (…) el medio no es el mensaje. El mensaje es el mensaje", ver [en línea], *lanación.com,* 26/12/2010.

(29) Palazzi, Pablo A., *op. cit.*, p. 75.

(30) Según el Diccionario de la Real Academia de Lengua Española: 1) Acción y efecto de comunicar o comunicarse; 2) Trato, correspondencia entre dos o más personas; y 3) Transmisión de señales mediante un código común al emisor y al receptor.

Volviendo al tratamiento dogmático de las figuras penales previstas en el art. 153 del CP, desde la perspectiva de los delitos informáticos, es menester señalar que esta disposición legal, en primer término, sanciona al que abriere o accediere indebidamente a una comunicación electrónica que no le esté dirigida.

En opinión de Arruvito:

> "... las comunicaciones electrónicas —que son el objeto protegido en la figura— se encuentran guardados, alojados, archivados, etc. en una cuenta de correo electrónico. O sea que para violentar la intimidad de la víctima, previamente debe tenerse acceso a la cuenta de ***e-mail.*** Recién una vez allí, el agresor podrá abrir, acceder, apoderarse, suprimir, desviar, interceptar o captar una comunicación electrónica".(31)

Vale aclarar que si bien esto puede suceder cuando se trata de correos electrónicos que funcionan bajo un protocolo SMTP,(32) existen otras comunicaciones electrónicas distintas del *e-mail* que no requieren, por así decirlo, de este paso previo.

Cabe señalar que **abre** quién descubre o hace patente aquello que está oculto, removiendo los obstáculos que lo cierran o protegen, a fin de impedir a terceros imponerse de su contenido; **accede** quien entra, ingresa u obtiene el objeto de protección legal. En este punto, corresponde hacer una distinción desde el sentido semántico de estos verbos típicos, pues bien podría decirse que un *e-mail* puede ser accedido aun cuando ya se encontrare abierto. Sin embargo, partiendo de la aclaración efectuada por el legislador respecto de la figura de "apoderamiento indebido de comunicaciones electrónicas" (**aunque no esté cerrado**) es posible sostener la interpretación contraria. Es decir, que en el acceso se requiere que las comunicaciones electrónicas estén cerradas;(33) no sería típica la conducta de

(31) Arruvito, Pedro A., "Ley 26.388. Violación del e-mail o comunicación electrónica", *Doctrina Judicial*, Bs. As., La Ley, 18/02/2009, p. 403.

(32) No así con el protocolo POP3, que funciona con programas como el Outlook, *Incredimail, Thunderbird, Windows Mail,* etc.

(33) Entiéndase por "cerradas", que para acceder, sea necesario iniciar una sesión y consecuentemente ingresar un nombre de usuario y contraseña.

la persona que se imponga del contenido de un correo electrónico o de un mensaje de texto, que ha quedado expuesto a la vista de terceros por un descuido de su titular.[34] Desde otro enfoque, se refiere que no queda en claro en qué se distinguen los verbos típicos abrir y acceder, y que respecto de este último podría decirse que el sujeto activo "… si bien llega a conocimiento del mail accedido, ello fue logrado sin haberlo abierto (puede ser porque no haya sido necesario 'abrir' el mail porque ya se encontraba abierto, o porque otra persona —la que sí lo abrió— se lo reenvió ya 'abierto')".[35] En síntesis, nos parece que la redacción legal no es clara, debiendo primar el criterio restrictivo por imperio del principio de legalidad. Por otro lado, bien podría afirmarse que un correo electrónico puede abrirse muchas veces porque las condiciones de seguridad que resguardan su contenido de la mirada de terceros (nombre de usuario, clave o contraseña, etc.), a diferencia del correo epistolar, carecen de soporte físico.[36]

Ahora bien, la apertura o el acceso de las comunicaciones electrónicas, debe realizarse **indebidamente**, es decir, sin derecho o autorización del titular. Según lo expresaba Molinario

> "... la voz indebidamente tiene más de un papel (…) Uno es recalcar que el dolo debe ser directo (…) Otro, que evidentemente no exista derecho a ejecutar esa acción. En primer lugar, por supuesto, tienen tal derecho las personas autorizadas por el destinatario. En general, los tribunales se han referido a este segundo aspecto tomando en cuenta diversos casos. Entre ellos, el de autorizaciones que diversas leyes[37] dan a ciertos funcionarios en casos determinados (hay autorizaciones administrativas, y por otro lado, judiciales) o el ejercicio de la patria potestad o de la tutela o curatela (…) o cuando entran en juego razones humanitarias…".[38]

(34) En contra de esta interpretación: Palazzi, Pablo A., *op. cit.*, p. 76/77.

(35) Arruvito, Pedro A., *op. cit.*

(36) A favor de la tesis según la cual la comunicación electrónica debe estar cerrada. Ver Ghersi, Sebastián, "Violación de secretos y privacidad. Los documentos electrónicos", en *Revista Jurídica La Ley*, 2008-F, p. 731.

(37) Por ejemplo: ley 25.520, ley 25.873, art. 236 CPPN, etc.

(38) Molinario, Alfredo J., *op. cit.*, p. 113.

En el mismo sentido, se pronuncia Palazzi quien entiende que la inclusión el término "indebidamente" tiene incidencia principalmente en la órbita del tipo subjetivo. De igual manera, se ha señalado que "con respecto al elemento subjetivo del tipo, la norma indica que el autor debe obrar a sabiendas o ilegítimamente, lo que significa saber claramente lo que hace o no hace y que ese hacer o no hacer es contrario a derecho. Estamos hablando de un dolo directo, no de uno indirecto o eventual".[39]

Sin embargo, creemos que esto se produce como un reflejo o consecuencia del juicio de tipicidad objetiva —función conglobante— en tanto el dolo exige el conocimiento y la voluntad de realización del tipo objetivo.[40] De esta manera, la exigencia típica opera por lógica sistemática al momento de analizar la eventual tipicidad objetiva de la conducta; es decir, este adverbio alude a la antinormatividad de la conducta, la que no se verificaría, por ejemplo, en caso de haber mediado el consentimiento del titular por ausencia de lesividad. Por lo demás, así como se ha criticado la voz "ilegítimamente" en el hurto (art. 162 del CP) por superflua, idéntica observación podría realizarse en este caso, aunque cabe aclarar que la inclusión del término obedeció principalmente al reclamo proveniente de empresarios del sector de la informática y las comunicaciones. Posiblemente hubiera sido preferible reemplazar el término en cuestión por la frase "violando sistemas de seguridad mínimos", siguiendo la línea ya trazada en el art. 1 inc. c) de la ley 24.766, respecto de la información confidencial, donde se requiere para su protección legal que dichos datos sean secretos, tengan valor comercial en función de la característica anterior y hayan sido objeto de medidas razonables, en las circunstancias, para mantenerlos así.

Finalmente, debe tratarse de una comunicación electrónica **que no le esté dirigida** al sujeto activo; dicho en otros términos, el autor de este delito no debe ser el destinatario de la comunicación electrónica, lo que en todo caso, se complementa con la exigencia de actuar en forma ilegítima.

(39) Romero, Rosario Margarita, Cámara de Diputados de la Nación, Secretaria Parlamentaria, Dirección de Información Parlamentaria, 34ª Reunión – 25ª Sesión Ordinaria, 11/10/2006 (versión taquigráfica).

(40) Esto según el finalismo y las teorías que resultan tributarias a esta escuela dogmática.

Párrafo aparte, merece la discusión que plantea el monitoreo de correos electrónicos en el ámbito laboral, donde las comunicaciones electrónicas se han transformado en un recurso casi indispensable en la mayoría de las actividades. En estos supuestos, coincidimos con la doctrina mayoritaria de que el usuario no tiene un derecho a la privacidad sobre estas comunicaciones, en tanto constituyen herramientas de trabajo; sin perjuicio de ello, sería conveniente que el empleador notifique a cada usuario (empleado) los términos y condiciones que rigen el uso de tales elementos en el ámbito estrictamente laboral, evitando así la generación de eventuales conflictos futuros. Siguiendo este criterio, se ha proyectado la incorporación del art. 86 *bis* a la ley 20.744 (LCT), proponiéndose el siguiente texto:

> "Cuando el correo electrónico sea provisto por el empleador al trabajador en función o con motivo de una relación laboral, se entenderá que la titularidad del mismo corresponde al empleador (…) El empleador se encuentra facultado para acceder y controlar toda la información que circule por dicho correo electrónico laboral, como asimismo a prohibir su uso para fines personales. El empleador no podrá prohibir el uso de las direcciones de correo electrónico que pudiera tener el trabajador que sean de carácter personal o privado, aunque los mismos sean abiertos desde el lugar de trabajo. El empleador deberá asimismo, notificar fehacientemente al empleado su política respecto del acceso y uso de correo electrónico personal en el lugar de trabajo, así como las condiciones de uso y acceso al correo electrónico laboral al momento de poner a su disposición el mismo…".(41)

La segunda conducta receptada en el primer párrafo del art. 153 del CP consiste en **apoderarse** indebidamente de una comunicación electrónica **aunque no esté cerrada**. Se apodera de un correo electrónico quién lo pone bajo su poder, se lo apropia o lo retiene en su ámbito de dominio. Compartimos con Palazzi que el término "apoderarse" no requiere aquí los requisitos típicos del hurto, pues cuando es aplicado a elementos digitales el sujeto activo puede realizar la conducta sin necesidad de des-

(41) Ver [En línea] http://www.iprofesional.com/notas/70004-Proyecto-de-ley.html. Nos parece que el art. 1 de este proyecto no regula con claridad el uso del correo electrónico de carácter personal o privado, como acontecía en el art. 4 de un proyecto de la Diputada Bisutti de fecha anterior (expte. 2032-D-06).

apoderar al damnificado, tal como ocurría con la copia o el reenvío de un e-mail. En estos casos habría apoderamiento, más no desapoderamiento en sentido estricto, dado que la comunicación original permanecería en la bandeja de entrada del correo electrónico del usuario.(42) A su vez, el sujeto activo podría apoderarse del correo electrónico mediante su impresión, en cuyo caso, se apropiaría de su contenido, afectando el derecho a la privacidad del sujeto pasivo, con la salvedad de que obtendría para sí una copia en soporte material del mismo, lo que entendemos no obsta a la configuración del delito. En sentido coincidente, en la Cámara de Diputados, en relación al texto legal se expuso que "el término apoderamiento debe entenderse en un doble sentido. Apoderarse de una comunicación electrónica puede ser copiarla o apoderarse físicamente de una copia".(43)

Por último, el párrafo bajo análisis, prevé una tercera y última figura básica: la supresión o el desvío indebido de comunicaciones electrónicas que no estén dirigidas al sujeto activo. **Suprime** quién hace desaparecer, destruye u oculta, impidiendo la circulación; mientras **desvía**, el que le da a la comunicación electrónica un curso distinto al estipulado por el remitente. En ambos supuestos, el sujeto activo altera el destino del *e-mail*, SMS, MMS, etcétera.

Como en el caso anterior, para la configuración del delito es requisito, por un lado, que la conducta sea realizada sin derecho (indebidamente), y por el otro, la ajenidad del correo electrónico. La intención del legislador ha sido dejar fuera del espectro de conductas incriminadas las prácticas de filtrado automático de comunicaciones electrónicas que realizan los ISP y las empresas proveedoras del servicio de correo electrónico, en pos de optimizar su rendimiento, eliminado SPAM, virus, etcétera. La Senadora Vilma Ibarra enfatizó que:

> "… hay que dejar en claro para la interpretación ulterior de los jueces en materia de interpretación auténtica a efectos de que no queden dudas a quienes interpretan la ley de que la finalidad debe ser dolosa; o sea, debe existir un dolo específico del

(42) Palazzi, Pablo A., *op. cit.*, p. 78.

(43) Romero, Rosario Margarita, Cámara de Diputados de la Nación, Secretaria Parlamentaria, Dirección de Información Parlamentaria, 35ª Reunión - 26ª Sesión Ordinaria, 25/10/2006 (versión taquigráfica).

> autor del delito (…) Muchas veces las empresas colocan filtros y desvían el spam, y esto no constituye la vocación dolosa de suprimirlo para causarle un daño al otro. Entonces, esto lo dejamos claramente especificado (…) la expresión indebidamente excluye, desde ya, la actividad empresarial para el desvío de spam".(44)

Debe distinguirse esta figura del denominado *sniffing* —derivado de la palabra *sniff*, que en inglés significa olfatear— donde no hay desvío de los paquetes de datos sino una triangulación entre ordenadores conectados a una misma red, a través de la cual es posible captar o acceder a esa información sin que emisor y destinatario lo adviertan. De esta forma, es posible apropiarse de claves, *e-mails*, y cualquier tipo de información, ya sea de carácter público o privado.

Justamente, el segundo párrafo del dispositivo legal en estudio castiga con prisión de quince días a seis meses al "… que indebidamente interceptare o captare comunicaciones electrónicas o telecomunicaciones provenientes de cualquier sistema de carácter privado o de acceso restringido".

Nuestra Constitución Nacional consagra expresamente la inviolabilidad de la correspondencia epistolar, pero por razones obvias, nada dice sobre la privacidad de las telecomunicaciones. En efecto, se ha señalado que "...la letra de la Constitución Nacional menciona solamente la privacidad de las comunicaciones epistolares: no pudo referirse a las comunicaciones telefónicas; pero es evidente que analógicamente cabe extender a estas la inviolabilidad prevista para aquellas…",(45) a lo que cabe agregar que "... ha sido voluntad de la ley 19.798 de telecomunicaciones que no sólo el intercambio epistolar quede en secreto, sino además la palabra transmitida por el cable telefónico (...) La ley 19.798 de telecomunicaciones se ha propuesto tutelar la personalidad integral del hombre a la luz del precepto constitucional del art. 18 …".(46)

(44) Ibarra, Vilma, Cámara de Senadores de la Nación, 18° Reunión (14° Sesión Ordinaria) 28 de noviembre de 2007, Versión Taquigráfica.

(45) Cám. Nac. Com., Sala D, mayo 18-1989, La Ley 1989-D-329.

(46) Cám. Nac. Crim. y Corr. , Sala VI, 04/11/1980, "Landeira de Ferradás, Josefina E.", La Ley 1981-B-193; JA 1981-II-333 y ED, 92-828.

En el derecho público provincial, hay disposiciones que expresamente protegen la privacidad de las comunicaciones telefónicas; tal es el caso, por ejemplo, de la Constitución de la provincia de San Luis.[47] Por su parte, nuestro Código Penal hasta la entrada en vigencia de la ley 26.388 no contenía disposición alguna que sancione la violación de las telecomunicaciones.[48]

En el plano normativo nacional, la ley 19.798 define el término **telecomunicaciones** como toda transmisión, emisión o recepción de signos, señales, escritos, imágenes, sonidos o informaciones de cualquier naturaleza, por hilo, radioelectricidad, medios ópticos u otros sistemas electromagnéticos (art. 2). Si bien esta ley no contiene disposiciones penales, establece que la correspondencia de telecomunicaciones es inviolable, procediendo su interceptación sólo a requerimiento de juez competente (art. 18) y que esta inviolabilidad importa la prohibición de abrir, sustraer, interceptar, interferir, cambiar su texto, desviar su curso, publicar, usar, tratar de conocer o facilitar que otra persona que no sea su destinatario conozca la existencia o el contenido de cualquier comunicación confiada a los prestadores del servicio y la de dar ocasión de cometer tales actos (art. 19).

Debe tenerse presente, además, la sanción de la ley 25.873 (BO 09/02/2004) en cuyo marco se ha establecido que todo prestador de servicios de telecomunicaciones:

> "… deberá disponer de los recursos humanos y tecnológicos necesarios para la captación y derivación de las comunicaciones que transmiten, para su observación remota a requerimiento del Poder Judicial o el Ministerio Público de conformidad con la legislación vigente. Los prestadores de servicios de telecomuni-

(47) Art. 33: "Los papeles particulares, la correspondencia epistolar, las comunicaciones telegráficas, telefónicas, teletipeado o de cualquier otra especie o por cualquier otro medio de comunicación, son inviolables y nunca puede hacerse registro de las mismas, examen o intercepción sino conforme a las leyes que se establecen para casos limitados y concretos. Los que son sustraídos, recogidos u obtenidos en contra de las disposiciones de dichas leyes, no pueden ser utilizados en procesos judiciales o administrativos".

(48) Creus, Carlos, "El miedo a la analogía...", *op. cit.* Antes de producirse el auge de la tecnología inalámbrica, sostenía que era aconsejable pero no imprescindible una reforma, ya que una conversación telefónica era confiada al cerramiento de un cable que valía (en cuanto a la tipicidad penal) como el sobre de una carta; de manera que quien penetraba aquél cerramiento lo "abría" y si lo hacía fuera de los supuestos autorizados lo hacía "indebidamente".

> caciones deberán soportar los costos derivados de dicha obligación y dar inmediato cumplimiento a la misma a toda hora y todos los días del año. El Poder Ejecutivo nacional reglamentará las condiciones técnicas y de seguridad que deberán cumplir los prestadores de servicios de telecomunicaciones con relación a la captación y derivación de las comunicaciones para su observación remota por parte del Poder Judicial o el Ministerio Público" (art. 45 *bis*).

Asimismos éstos:

> "…deberán registrar y sistematizar los datos filiatorios y domiciliarios de sus usuarios y clientes y los registros de tráfico de comunicaciones cursadas por los mismos para su consulta sin cargo por parte del Poder Judicial o el Ministerio Público de conformidad con la legislación vigente. La información referida en el presente deberá ser conservada por los prestadores de servicios de telecomunicaciones por el plazo de diez años" (art. 45 *ter*).

Además, en el art. 45 *quater* se introduce una cláusula de naturaleza resarcitoria mediante la cual el Estado Nacional asume responsabilidad por los eventuales daños y perjuicios que pudieran derivarse para terceros.

Posteriormente, desde la óptica de la protección del derecho constitucional a la intimidad y a la vida privada, la situación se vio agravada a raíz del dictado del decreto reglamentario 1563/2004 —suspendido por el decreto PEN 357/2005—, finalmente declarado inconstitucional por el Máximo Tribunal de la República, en el caso "Halabi, Ernesto c/PEN ley 25.873 dto. 1563/04 s/ amparo ley 16.986", del 24/02/2009. En este pronunciamiento, la Corte definió y precisó los alcances de los derechos de incidencia colectiva referentes a intereses individuales homogéneos,[49] y

(49) Estos derechos surgen del segundo párrafo del art. 43 de nuestra Carta Magna. En particular se dijo que: "... en estos casos no hay un bien colectivo, ya que se afectan derechos individuales enteramente divisibles. Sin embargo, hay un hecho, único o continuado, que provoca la lesión a todos ellos y por lo tanto es identificable una causa fáctica homogénea. Ese dato tiene relevancia jurídica porque en tales casos, la demostración de los presupuestos de la pretensión es común a todos esos intereses, excepto en lo que concierne al daño que individualmente se sufre. Hay una homogeneidad fáctica y normativa que lleva a considerar

señaló a las **acciones de clase** como el medio o carril procesal idóneo para canalizar jurisdiccionalmente la defensa de estos intereses. Al mismo tiempo, y en relación a la cuestión de fondo, destacó que: "… el Tribunal Constitucional de España, mediante su sentencia del 5 de abril de 1999 (STC 49/1999), con cita del Tribunal Europeo de Derechos Humanos (TEDH), ha sostenido que 'si el secreto pudiera alzarse sobre la base de meras hipótesis subjetivas, el derecho al secreto de las comunicaciones (...) quedaría materialmente vacío de contenido…"; y que:

> "... es evidente que lo que las normas cuestionadas han establecido no es otra cosa que una restricción que afecta una de las facetas del ámbito de la autonomía individual que constituye el derecho a la intimidad, por cuanto sus previsiones no distinguen ni precisan de modo suficiente las oportunidades ni las situaciones en las que operarán las interceptaciones, toda vez que no especifican el tratamiento del tráfico de información de Internet en cuyo contexto es indiscutible que los datos de navegación anudan a los contenidos. Se añade, a ello, la circunstancia de que las normas tampoco prevén un sistema específico para la protección de las comunicaciones en relación con la acumulación y tratamiento automatizado de los datos personales. En suma (…) resulta inadmisible que las restricciones autorizadas por la ley estén desprovistas del imprescindible grado de determinación que excluya la posibilidad de que su ejecución concreta por agentes de la Administración quede en manos de la más libre discreción de estos últimos, afirmación que adquiere primordial relevancia si se advierte que desde 1992 es la Dirección de Observaciones Judiciales de la SIDE, que actúa bajo la órbita del poder político, la que debe cumplir con los requerimientos que formule el Poder Judicial en orden a la interceptación de comunicaciones telefónicas u otros medios de transmisión que se efectúen por esos circuitos".[50]

razonable la realización de un solo juicio con efectos expansivos de la cosa juzgada que en él se dicte, salvo en lo que hace a la prueba del daño" (consid. 12 del voto de la mayoría).

(50) Consids. 24 y 26 del voto de la mayoría, suscripto por los Ministros Lorenzetti, Higthon de Nolasco, Maqueda y Zaffaroni.

Luego de esta introducción, daremos paso al análisis de los requisitos típicos de esta figura. Incurre en este delito quien sin autorización **intercepta** (se apodera, detiene, obstruye, o interrumpe una vía de comunicación) o **capta** (percibe, obtiene, recoge) comunicaciones electrónicas o telecomunicaciones de carácter privado o de acceso restringido. La técnica legislativa empleada es criticable, pues no resultará tarea sencilla distinguir (si es que esa fue la intención del codificador penal) entre, por un lado, comunicaciones electrónicas y telecomunicaciones, y por el otro, sistema de carácter privado y sistema de acceso restringido. En primer término, porque el art. 77 del CP no establece una definición de "comunicación electrónica" y atento la amplitud otorgada al término "telecomunicación" en la ley 19.798, este último concepto parece abarcar al primero. Así, en el Informe Preliminar de la Comisión de Estudio de Correo Electrónico, elaborado en el ámbito de la Secretaría de Comunicaciones, dependiente del Ministerio de Infraestructura y Vivienda, de fecha 07/08/2001, se explicaba que:

> "... el diccionario general de la lengua española define el termino correo electrónico como correspondencia que se transmite por un ordenador a un usuario concreto. Es esta la acepción que receptamos en el presente anteproyecto de ley que sometemos a consideración, haciendo especial referencia a que solo se considera correo electrónico al que se transmite por medio de una red de interconexión entre computadoras, excluyendo del ámbito de esta ley a cualquier otra modalidad de mensaje transmitido por medios electrónicos, como por ejemplo los emitidos a través del servicio de radiocomunicaciones para ser receptados por un móvil portátil (pager) o los recibidos a través del servicio de audio texto".(51)

No obstante, esa distinción no se aplica al término "comunicación electrónica", que claramente incluye, como ya hemos visto, SMS, MMS, logs de chat, mensajes de voz por redes IP, etc.(52) Y en segundo término, no se

(51) [En línea] www.zendo.com.ar/documentos/Informe_Preliminar.doc

(52) En relación a las vulnerabilidades que presentan las redes de telefonía celular, como las prácticas más usuales de escuchas, puede consultarse: Kanto, Damián, "Privacidad en peligro. Para escuchar conversaciones usan celulares como micrófono", Clarin.com, 22/04/1998. En este artículo, entre otras cosas, se explica que "… existen distintas maneras de acceder a

aprecian con facilidad las diferencias existentes entre sistemas privados o de acceso restringido, y en todo caso, ello da lugar a distintas interpretaciones. De nuestra parte, coincidimos con Palazzi que será de acceso restringido en cuanto tenga alguna medida de seguridad que impida el libre acceso.(53) Resulta innegable que "... no son objeto del delito las de carácter público, no en el sentido de servicio público, sino en el de que la comunicación no es privada sino abierta, tales como un mensaje subido a un blog que puede leer cualquiera…".(54) Entonces, deben tratarse de sistemas cerrados, resultando la información que allí circula de carácter privado (personal), o bien, no destinada a ser conocida por terceros. También podría tratarse de información confidencial por aplicación de la ley 24.766 (arts. 1, 2 y 12).

Cabe aclarar que en esta figura el objeto de protección son "sistemas informáticos privados o de acceso restringido", resultando excluidos los pertenecientes a un banco o archivo de datos personales (art. 157 *bis* del CP), cuyas características particulares están prefijadas en la ley 25.326. En otras palabras, puede tratarse de una PC o de una red compuesta por varios dispositivos electrónicos. A su vez, es fácil de imaginar la posibilidad

conversaciones ajenas (…) las modalidades dependen de varios factores: el tipo de aparato celular, el tipo de escucha que se pretende y la distancia del individuo que posee la terminal. Para entender cómo se realizan estas acciones, es preciso saber —aunque sea de manera superficial— cómo funciona la red de telefonía celular. La red tiene un complejo tramado de antenas. Cada una funciona como receptor y transmisor de señal de voz. Las antenas reciben el nombre de celda o célula (de ahí la denominación celular) y tienen un alcance de aproximadamente 20 manzanas. Este es el radio de alcance, aunque depende de la zona en que esté instalada. Cuando un usuario tiene encendido su aparato telefónico se vincula con la celda más cercana enviando dos códigos que tiene el celular: el ESN (*Electronic Serial Number*, que es una clave interna del aparato) y el MIN (*Movil Identification Number*) que es el número telefónico asignado por la prestadora del servicio. Esto permite al sistema informático de la empresa, ubicar al usuario y saber su posición. El sistema celular funciona a través de frecuencias de radio. Cuando se mantiene una conversación, la señal se envía a determinada frecuencia. El que dispone de esa información y tiene el equipo adecuado para interferirla, puede escucharla. Para detectarla se valen de unos aparatos llamados escáner que localizan la frecuencia de la víctima (…) Un espía que tiene los códigos, la frecuencia y la tecnología para efectuar la pinchadura, tiene que estar sí o sí en la misma celda o antena que el blanco. (…) Sin embargo, las modalidades de pinchaduras más difundidas en el mundo y en la Argentina no se limitan al ejemplo anterior. El más llamativo es el que permite usar un aparato celular de un usuario como si fuera un micrófono ambiente".

(53) Palazzi, Pablo A., *op. cit.*, p. 102.

(54) *Ibid.*, p. 82.

de un concurso ideal con el delito previsto en el artículo en el art. 153 *bis* del digesto punitivo.

En el plano subjetivo, estamos aquí también ante un delito doloso (directo), que admite la tentativa. Sobre el particular, nos remitidos a las consideraciones efectuadas al analizar los tipos penales de violación, apoderamiento, supresión y desvío de la correspondencia y los papeles privados.

Por último, la ley 26.388 omitió toda regulación legal de las cámaras ocultas, frecuentemente utilizadas en investigaciones periodísticas, con el argumento de que, de lo contrario, era posible afectar la libertad de expresión, optándose entonces por diferir su tratamiento para otra ocasión, lo que hasta el presente no ha ocurrido.(55) En la Cámara Alta también se sostuvo que esta cuestión no tenía que ver específicamente con los Delitos Informáticos.

Ahora bien, el art. 153 del CP agrava las penas previstas para las figuras básicas en dos casos:

a. "…si el autor además comunicare a otro o publicare el contenido de la carta, escrito, despacho o comunicación electrónica" la pena será de prisión de un (1) mes a un (1) año".

Comunicar es transmitir, hacer saber o dar a conocer a un tercero o terceros, distintos del destinatario, mientras publicar, es revelar, hacer notorio o difundir a un número indeterminado de personas el contenido de la comunicación electrónica.(56)

En general como lo ha destacado la doctrina este delito se configura en dos actos, pues presupone la existencia previa de alguno de los delitos previstos en los párrafos anteriores (apertura o acceso; apoderamiento;

(55) Se discutió la incorporación al Código Penal del art. 153 *ter*, bajo la siguiente redacción: "Será reprimido con prisión de un mes a dos años, el que ilegítimamente y para vulnerar la privacidad de otro, utilizando mecanismos de escucha, intercepción, transmisión, grabación o reproducción de voces, sonidos o imágenes, obtuviere, difundiere, revelare o cediere a terceros los datos o hechos descubiertos o las imágenes captadas" (Cámara de Diputados de la Nación, OD Nº 1227, 26/10/2006).

(56) Ver, Navarro, Guillermo R.; Báez, Julio C.; Aguirre, Guido J., "*Violación de Secretos y de la Privacidad*", en David Baigún y Eugenio Raúl Zaffaroni (dir), *Código Penal y normas complementarias. Análisis doctrinal y jurisprudencial*, Bs. As., Hammurabi, 2008, p. 724.

supresión o desvío; interceptación o captación de comunicaciones electrónicas). Para Grasso: "... la forma agravada remite a las manifestaciones típicas expuestas, con la sola excepción del desvío de correspondencia. La exclusión responde al principio que proscribe la doble valoración de los elementos del tipo penal, pues el desvío implica ya el conocimiento del contenido a manos de un falso destinatario".(57)

b. "... 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".

Por el término "funcionario público" o "empleado público" se designa a todo el que participa accidental o permanentemente del ejercicio de funciones públicas, sea por elección popular o por nombramiento de autoridad competente (art. 77 del CP).(58) Asimismo, la función de la cual se abusa debe dar ocasión o favorecer en modo alguno la realización de cualquiera de las conductas precisadas en las figuras básicas.

Si el funcionario público perteneciere al Sistema de Inteligencia de la Nación rige la ley 25.520, que en su art. 5°, establece que:

> "... las comunicaciones telefónicas, postales, de telégrafo o facsímil o cualquier otro sistema de envío de objetos o transmisión de imágenes, voces o paquetes de datos, así como cualquier tipo de información, archivos, registros y/o documentos privados o de entrada o lectura no autorizada o no accesible al público, son inviolables en todo el ámbito de la República Argentina, excepto cuando mediare orden o dispensa judicial en sentido contrario".

Consecuentemente, en los arts. 42 y 43 prevé disposiciones penales para aquellos agentes de la Secretaría de Inteligencia del Estado (SIDE) que se aparten de sus obligaciones funcionales. Así, incurrirá en delito, la persona que participando en forma permanente o transitoria de las tareas reguladas en dicha ley, indebidamente interceptare, captare o desviare comunicaciones telefónicas, postales, de telégrafo o facsímil, o cualquier

(57) Grasso, Mariana, "Violación de Secretos", en Luis Niño y Stella Maris Martínez, (coords.) *Delitos contra la Libertad*, 2° ed., Bs. As., Ad-Hoc, 2010, p. 358.

(58) Ver también la Ley 25.188 de Ética de la Función Pública.

otro sistema de envío de objetos o transmisión de imágenes, voces o paquetes de datos, así como cualquier otro tipo de información, archivo, registros y/o documentos privados o de entrada o lectura no autorizada o no accesible al público que no le estuvieren dirigidos. Finalmente, también sanciona con pena de prisión e inhabilitación especial al que con orden judicial y estando obligado a hacerlo, omitiere destruir o borrar los soportes de las grabaciones, las copias de las intervenciones postales, cablegráficas, de facsímil o de cualquier otro elemento que permita acreditar el resultado de las interceptaciones, captaciones o desviaciones.

5.2 | Artículo 153 *bis* del Código Penal

La ley 26.388 incorporó al catálogo punitivo el tipo penal que, a continuación, se transcribe:

> "Será reprimido con prisión de quince días a seis meses, si no resultare un delito más severamente penado, el que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido.
>
> La pena será de un mes a un año de prisión cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros".

Se trata de una figura de aplicación subsidiaria, y por lo tanto, será desplazada si la conducta imputada recayera en un delito más severamente penado.

Mucho se ha dicho alrededor de los reparos que presenta este tipo penal a la luz de los principios de mínima intervención, subsidiariedad del derecho penal, exclusiva protección de bienes jurídicos y *ultima ratio*. Su construcción político criminal responde a los estándares del denominado proceso de Modernización del Derecho Penal, en el cual la función y los límites del "viejo" derecho penal liberal parecen debilitarse. En efecto, esta tendencia político criminal punitivista o neopunitivista ha sido denominada Derecho Penal de Segunda Velocidad (Silva Sánchez) o Derecho

de Intervención (Hassemer), y por su intermedio, se pretende replantear las bases filosóficas y políticas del derecho penal liberal.[59] Conforme a esta nueva orientación, el **derecho penal de riesgos**"[60] requiere de instrumentos jurídico-penales flexibles, que reemplacen los rígidos principios del sistema de garantías de la Ilustración, pues así el Estado será capaz de proteger a la sociedad de los múltiples y novedosos riesgos humanos que la acechan a la luz del auge tecnológico y la complejización de la vida en comunidad. Ejemplo paradigmático de esta clase de legislaciones, es el Código Penal Español de 1995, siendo aún más intenso el declive de garantías en la legislación antiterrorista y el derecho penal internacional (Derecho Penal de Cuarta Velocidad). En este marco, se alude, por ejemplo, a un concepto formal de **bien jurídico** o a la anticipación de la tutela penal en virtud de exigencias o consideraciones político-criminales de corte preventivo. El fundamento detrás de la incriminación de estas conductas reside en su consideración como actos previos o antesala de delitos más graves, como defraudaciones y estafas, ofensas al honor, y otros. En este sentido, la prestigiosa doctrina afirma que estas conductas carecen de entidad suficiente en términos de lesividad para legitimar la intervención del derecho penal, resultando preferible la vía contravencional, o en todo caso, su incriminación bajo la amenaza de imposición con penas distintas a la privativa de libertad, como multa, inhabilitación especial o alternativas reparatorias.[61] Por otro lado, se ha referido con justeza que "resulta inaceptable suplantar las deficiencias procesales del sistema mediante la inclusión de un tipo penal que prevé esta conducta como delito autónomo justamente por no poder acreditar ultra finalidad

(59) A modo de ejemplo, los Códigos Penales de la primera mitad del siglo pasado, apenas tenían un par de delitos de peligro, dejando las conductas sin resultado concreto como delitos tentados, con la consiguiente reducción de la escala penal. Hoy día, en cambio, los delitos de peligro y los tipos de omisión impropia se multiplican y justifican mediante la invocación de necesidades político-criminales.

(60) La "Escuela de Frankfurt", iniciada por los profesores Wolfang Naucke, Klaus Lüderssen y Winfried Hassemer, se ha constituido en la principal usina crítica al cambio de dirección del derecho penal orientado principalmente a las consecuencias. Muy ilustrativo sobre este tema resulta el libro de AAVV, *Crítica y Justificación del Derecho Penal en el Cambio de Siglo. El análisis crítico de la Escuela de Frankfurt*, Cuenca, Colección Estudios, Ediciones de la Universidad de Castilla - La Mancha, 2003.

(61) Riquert, Marcelo A., *Delincuencia Informática. En Argentina y el Mercosur*, Bs. As., Ediar, 2009, p. 182.

o como adelantamiento de la barrera punitiva y por ende disminuyendo el ámbito de libertad de las personas".(62)

Sujeto activo de este delito puede ser cualquier persona, y ésta debe **acceder** (entrar, ingresar u obtener) al objeto de protección legal conforme las modalidades típicas que veremos a continuación. A fin de llevar adelante la finalidad ilícita el autor puede realizar el **acceso por cualquier medio,** es decir, el ingreso u obtención de un sistema o dato informático, puede efectuarse en forma directa o remota. Así, existen diversos recursos para procurar este cometido, basta mencionar sólo algunos de ellos: a) *malware*, que tiene como objetivo infiltrarse en una computadora a través de virus, gusanos, troyanos, bombas de tiempo o lógicas, *rootkits*, *keyloggers*, y otros software maliciosos; b) *cookies*, es decir, fragmentos de información que se almacenan en el disco duro del visitante de una página web a través de su navegador, a petición del servidor de la página, resultando posible conseguir información sobre los hábitos del usuario; c) *spyware*, es decir, programas espías cuya finalidad es hurgar en la información de un ordenador, en búsqueda de algún dato privado; d) ingeniería social, consistente en la obtención de información confidencial de manos del propio usuario, a través de técnicas de manipulación o engaño, etcétera.

La ley 25.326 define **datos informatizados** como los datos personales —información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables— sometidos al tratamiento o procesamiento electrónico o automatizado. Compartimos que, a los efectos de la interpretación de los alcances del art. 153 *bis*, "no debe tratarse necesariamente de un dato personal".(63) No obstante, reafirmamos que es necesario delimitar el ámbito de aplicación del tipo en función del bien jurídico tutelado, de forma tal que el dato, amén de ser de acceso restrin-

(62) Rosende, Eduardo, "El intrusismo informático. Reflexiones sobre su inclusión al código penal", Ponencia presentada en el VII Encuentro de la AAPDP realizado en la Facultad de Derecho de la Universidad de Buenos Aires, los días 7, 8 y 9 de noviembre de 2007. De este autor, véase también, *Derecho Penal e Informática. Especial referencia a las amenazas lógico informáticas*, Bs. As., Fabián Di Plácido, 2007.

(63) Palazzi, Pablo A., *op. cit.*, p. 103.

gido, debe revestir el carácter de secreto o privado.[64] En otras palabras, no cualquier dato reúne las características típicas, aunque lógicamente pueda configurarse el delito —con independencia de las cualidades del dato— desde el momento en que se acceda al sistema informático de acceso restringido (sin autorización) que eventualmente lo contenga. Nuevamente aquí, debe tenerse presente lo establecido en el art. 12 de la ley 24.766 respecto de la confidencialidad de la información comercial.[65]

Por su parte, el Convenio sobre la Ciberdelincuencia del Consejo de Europa, instrumento jurídico tenido en cuenta por el legislador nacional como importante antecedente de derecho internacional, define al "sistema informático", como todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, siempre que uno o varios de ellos permitan el tratamiento automatizado de datos en ejecución de un programa (art. 1, letra a). Asimismo, al tratarse de un sistema informático o dato de acceso restringido se requiere que el usuario o el administrador de la Red hayan adoptado alguna medida de seguridad, por mínima que sea. Principalmente, y por sentido inverso, no debe poder accederse al objeto de protección legal en forma libre o irrestricta; en otras palabras, por su disposición no debe estar destinado a ser accedidos por terceros no autorizados. Al respecto, se ha señalado que:

> "... el término restringido no es muy feliz y hubiera sido mejor que el legislador describiera la situación en que debían encontrarse el sistema o dato informáticos (por ejemplo, porque tiene medidas de seguridad que lo amparan) (…) no debe entenderse como un elemento fáctico, sino como uno normativo del tipo penal (…) está orientado a resaltar la obligación de no ingresar en un ordenador extraño".[66]

(64) Amans, Carla V. y Nager, Horacio S., *Manual de Derecho Penal. Parte Especial*, Bs. As., Ad-Hoc, 2009, p. 214.

(65) Con mayor claridad, el art. 197 del Código Penal Español establece que: "1. El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses…".

(66) Palazzi, Pablo A., *op. cit.*, p. 103.

Es de destacar, en relación con lo anterior, que al no exigirse un umbral o nivel mínimo de seguridad informática, cualquier sistema o dato informático de acceso restringido, aún el más vulnerable, sería típico.(67) En todo caso, será tarea de la jurisprudencia analizar, en el caso concreto, la entidad de la conducta y la incidencia del comportamiento de la víctima, en el estrato analítico de la tipicidad o en la determinación judicial de la pena.

Antes de la sanción de la Ley de Delitos Informáticos, mucho se discutió acerca de las diferencias entre el intrusismo informático blanco o ético, de aquel que no lo es. Así se explicaba que el primero procura poner a prueba la seguridad de un sistema informático para descubrir sus vulnerabilidades, sin otra intención subyacente que la optimización del mismo. En cambio, el *hacking* no ético es realizado con una ultrafinalidad delictiva. Atento a la redacción típica, el mero intrusismo informático sería típico; no obstante, debe tenerse especialmente en cuenta al bien jurídico protegido para evitar caer en procesos de criminalización irrazonables (arts. 19 y 28 CN).(68) Claro está, que el problema del *ethical hacking* se presenta cuando el intruso actúa sin el consentimiento o la autorización del titular del sistema o dato informático explorado.

El sujeto activo debe realizar la conducta "a sabiendas", lo que conduce a la exigencia de un dolo directo. Riquert señala que "se trata de un delito doloso, que por este condicionamiento subjetivo es sólo compatible con el dolo directo, excluyendo el eventual, dejando por fuera la punición de todo acceso fortuito, casual o imprudente".(69) Además, se debe actuar

(67) El Convenio sobre la Ciberdelincuencia del Consejo de Europa Budapest - 2001 establece que cada Estado Parte tipificará como delito en su derecho interno el acceso deliberado e ilegítimo a la totalidad o a una parte de un sistema informático, pudiendo exigir que este delito se cometa infringiendo medidas de seguridad, con la intención de obtener datos informáticos o con otra intención delictiva, o en relación con un sistema informático que esté conectado a otro sistema informático.

(68) Tal sería el caso de un proceso penal, de alta exposición mediática, sustanciado en EEUU a principios de la década de 1990, que culminó en la condena de integrantes de un grupo de *hackers* denominado LOD (*Legión of Doom*) por realizar actividades supuestamente peligrosas, como haber ingresado a un servidor privado y apoderarse de un documento cuyo nombre era "E91", que en realidad contenía información respecto del sistema de emergencias de la empresa AT&T, de conocimiento público (ver Rosende, Eduardo, "*El intrusismo informático. Reflexiones sobre su inclusión al código penal*", Ponencia presentada en el VII Encuentro de la AAPDP realizado en la Facultad de Derecho de la Universidad de Buenos Aires, los días 7, 8 y 9 de noviembre de 2007.

(69) Riquert, Marcelo A., *Delincuencia Informática, op. cit.* p. 181.

"sin la debida autorización o excediendo la que se posea", lo que equivale, en pocas palabras, a hacerlo sin derecho o indebidamente. Esto se daría, por ejemplo, "en los casos del personal de una institución autorizado para acceder sólo a determinados datos o archivos y que violando directivas internas, accede a sistemas, datos o archivos a los cuales no tiene acceso autorizado".(70) Por supuesto, que si el titular del sistema o dato informático permite el acceso, no estaremos ante un delito, no requiriendo dicha autorización formalidad alguna, más allá de que por razones de índole probatoria sea recomendable tomar recaudos al respecto.

La pena se agrava cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal —ANSES, AFIP, BCRA, IGJ, Dirección Nacional de Migraciones, Registro Nacional de Reincidencia y Estadística Criminal, etcétera— o de un proveedor de servicios públicos o de servicios financieros —Colegio Público de Abogados de la Capital Federal, Colegio de Escribanos de la Ciudad de Buenos Aires, Bancos y Entidades Financieras, Registro de la Propiedad Inmueble de la Ciudad de Buenos Aires, etcétera—. Puede tratarse de entes de derecho público centralizados o descentralizados, autárquicos o autónomos, y también de personas de existencia ideal de carácter privado que suministren o proveen un servicio público, tales como empresas concesionarias, bancos y demás entidades financieras, etcétera. La razón de la agravante reside en la naturaleza pública del sistema o dato informático accedido. En este punto, cabe aclarar que el acceso recaerá sobre el sistema informático perteneciente a cualquiera de estos entes jurídicos, más el dato allí contenido, si se refiere a condiciones inherentes a un usuario en particular: —vulnerará también un interés subjetivo individual—.

Si nos atenemos a la letra de la ley, es un delito de acción privada por imperio de lo establecido en el art. 73 inc. 2 del CP, lo que presenta algunas dudas, especialmente en lo referente a la figura calificada. Parte de la doctrina sostiene que esto obedece a un olvido legislativo; mientras otro sector, entiende que la exclusión es correcta, ya que los titulares de esos datos privados, confidenciales o secretos, son personas físicas o jurídicas puntualmente damnificadas.

(70) Arruvito, Pedro A., *op. cit.*

5.3 | Artículo 155 del Código Penal

La disposición legal reprime con multa (de pesos un mil quinientos a pesos cien mil) a la persona 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"; especificando, en un segundo párrafo, que "está exento de responsabilidad penal el que hubiere obrado con el propósito inequívoco de proteger un interés público".

Para la consumación del delito no es suficiente la simple comunicación del contenido a un tercero o terceros determinados, tal como lo admite la redacción del art. 153 del CP; este tipo penal exige que la comunicación electrónica sea publicada, es decir, que sea puesta en conocimiento del público en general, expuesta a un número indeterminado de personas. Resultan indiferentes los medios comisivos, pudiendo el autor realizar la publicación por sí mismo o a través de un tercero (editor, director de un periódico, blogger).

Además, el sujeto activo debe hallarse en posesión de la comunicación electrónica —sea porque se trate del destinatario o por cualquier otra razón— en forma lícita, ya que de lo contrario, resultaría de aplicación la agravante prevista en el art. 153 del CP. En otros términos, no se requiere ninguna cualidad especial para ser autor, pero la posesión de la comunicación electrónica debe haberse adquirido en forma legítima, resultando desvalorada aquí la conducta de hacer público su contenido cuando la misma no estaba destinada a trascender a un número indeterminado de individuos.

No es un delito de resultado, por lo que basta la existencia de un perjuicio potencial, el que puede asumir cualquier naturaleza —material, moral, patrimonial, etcétera—, pero este debe ser consecuencia directa del hecho de la publicación abusiva.[71] El comportamiento debe llevarse adelante con conocimiento y voluntad de realización del tipo objetivo,

(71) Fontán Balestra, *Derecho Penal. Parte Especial*, actualizado por Guillermo A. C. Ledesma, 16° ed., Bs. As., Lexis-Nexis - Abeledo-Perrot, 2002, p. 372. En igual sentido ver Navarro, Guillermo R.; Báez, Julio C. y Aguirre, Guido J., *op. cit.*, p. 760.

por lo que se requiere obrar con dolo (directo). Admite la tentativa. Finalmente, la ley 26.388, exime de responsabilidad a quien obre con el propósito inequívoco de proteger un interés público.

5.4 | Artículo 157 del Código Penal

El art. 157 del CP reprime, con penas de prisión de un mes a dos años e inhabilitación especial de uno a cuatro años, al "funcionario público que revelare hechos, actuaciones, documentos o datos, que por ley deben ser secretos".

Se trata del delito de violación de Secreto Oficial, no habiendo la ley 26.388 de Delitos Informáticos introducido modificaciones sustanciales, dado que el legislador se limitó a actualizar el texto legal mediante la incorporación de la voz "datos", que debe entenderse en sentido amplio, conforme fuera desarrollado precedentemente al analizar la estructura típica del delito de intrusismo informático (art. 153 *bis* del CP).

El sujeto activo debe presentar una cualidad específica: ser funcionario público (art. 77 del CP), y en virtud de esta condición especial, debe recaer en su persona la obligación legal de guardar secreto sobre los datos que hubiere conocido en ejercicio o en ocasión de sus funciones. La obligación de guardar el secreto debe ser impuesta por la ley (art. 51 del CP), de manera que el funcionario, al quebrantarlo, no sólo vulnera un deber genérico de confianza y privacidad, sino que su acción deviene antinormativa, al contradecir una disposición legal que expresamente lo obliga a guardar silencio.

Esta figura será desplazada en caso de concurrir, en el supuesto de hecho, los requisitos típicos contemplados en los arts. 222 y 223 del CP, o en los arts. 2 y 3 de la ley 13.985, también conocida como Ley Antiespionaje. A su vez, compartimos que "en caso de que un funcionario público revelare ilegítimamente un secreto oficial que fuera a su vez información personal registrada en un banco de datos personales, el tipo penal del art. 157 del CP —que releva que el secreto concierna a las esferas de actuación del Estado— será el que prevalezca".[72]

(72) Seco Pon, Juan Carlos, "Violación de datos personales (art. 157 bis, CP) y revelación de secretos oficiales (art. 157, CP)", en Niño, Luis y Martinez, Stella Maris (coords.), *op. cit.*, p. 570.

El delito se consuma cuando el secreto es revelado, lo que equivale a su comunicación a un sujeto que no está autorizado a conocerlo; quien incluso pude también revestir la calidad de funcionario público. El delito es doloso, discutiéndose en la doctrina si basta con el dolo eventual, o si éste debe ser directo.(73) Admite la tentativa.

Por encontrarse en juego un interés público, parece razonable su inclusión en el catálogo de delitos perseguibles de oficio (arts. 71 y 73 inc. 2 del CP).

5.5 | Artículo 157 *bis* del Código Penal

Los datos personales no son una novedad, más lo que provoca alarma en la actualidad es su facilidad de obtención, almacenamiento, tratamiento y divulgación. A diferencia de lo que acontecía con el viejo fichero, la capacidad de almacenamiento y tratamiento de información hoy es inmensa, su consulta es sumamente sencilla, y no está sujeta a las restricciones o limitaciones temporales y espaciales tradicionales. El resultado del procesamiento de estos datos se obtiene en forma casi inmediata, constituyendo una herramienta de enorme utilidad, y a la vez económica, por el ahorro de energía y de recursos humanos que posibilita. Sin embargo, este inconmensurable caudal de información, puesto a disposición del gobierno o de particulares, presenta un grave riesgo a la esfera de intimidad de las personas. Es que en la "sociedad de la información", más que nunca, es necesario responder al interrogante relativo a qué se debe guardar y qué no, con qué fines y por cuánto tiempo.

Consideramos que el análisis de esta disposición debe ser precedido por una breve remisión al contenido de la ley 25.326 de *Hábeas Data* (BO 02/11/2000), reglamentaria del instituto previsto en la Ley Fundamental.(74) Este cuerpo legal establece que su objeto es la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes, para garantizar el derecho al

(73) Navarro, Guillermo R.; Báez, Julio C. y Aguirre, Guido J., *op. cit.*, p. 802.

(74) Esto, sin desconocer que "las garantías constitucionales existen y protegen a los individuos por el solo hecho de estar en la Constitución e independientemente de sus leyes reglamentarias, cuyas limitaciones no pueden constituir obstáculo para la vigencia efectiva de dichas garantías" (Fallos: 239:459; 241:291 y 315:1492).

honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre, de conformidad a lo establecido en el art. 43, párr. tercero de la Constitución Nacional. Y agrega, que sus disposiciones también serán aplicables, en cuanto resulte pertinente, a los datos relativos a personas de existencia ideal, y que en ningún caso, se podrán afectar la base de datos ni las fuentes de información periodísticas (art. 1).

En el art. 2, se definen diversos términos, lo que contribuye a una correcta hermenéutica del texto legal. De esta manera, se precisa qué debe entenderse por datos personales; datos sensibles; archivo, registro, base o banco de datos; tratamiento de datos; responsable de archivo, registro, base o banco de datos; datos informatizados; titular de los datos; usuario de datos; y disociación de datos. Particular importancia reviste la distinción entre **datos personales** —o sea, información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables—y **datos sensibles** —es decir, datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual—.

Por su parte, en el art. 5, se establece que el tratamiento de datos personales, sólo será lícito cuando el titular lo consintiera en forma libre, expresa e informada, documentándose por escrito, o por otro medio que se le equipare. Así, la regla es que debe solicitarse el consentimiento del titular de los datos, admitiendo las siguientes excepciones: a) datos obtenidos de fuentes de acceso público irrestricto; b) datos que se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal; c) listados cuyos datos se limiten a nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio; d) datos que deriven de una relación contractual, científica o profesional del titular de los datos, y resulten necesarios para su desarrollo o cumplimiento; e) operaciones que realicen las entidades financieras e informaciones que reciban de sus clientes, conforme las disposiciones del art. 39 de la ley 21.526.

La Dirección Nacional de Protección de Datos Personales es el órgano de control creado en el ámbito Nacional para la efectiva protección de los datos personales, que tiene a su cargo el Registro de las Bases de Datos,

debiendo asesorar y brindar asistencia a los titulares de datos personales ante denuncias y reclamos efectuados contra los responsables de los registros, archivos, bancos o bases de datos, por violación de los derechos de información, acceso, rectificación, actualización, supresión y confidencialidad en el tratamiento de los datos.

Ahora bien, el art. 157 *bis* reprime con pena de prisión de un mes a dos años a la persona que realice cualquiera de estas conductas: 1) Acceso ilegítimo a un banco de datos personales; 2) Revelación de secretos registrados en un banco de datos personales; 3) Inserción de datos en un banco de datos personales. A continuación, veremos cada una de ellas.

En el inc. 1 se reprime a la persona que "a sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales".

Sujeto activo del delito es quien accede a un banco de datos personales "a sabiendas e ilegítimamente" o "violando sistemas de confidencialidad y seguridad de datos", pudiendo servirse de cualquier medio para alcanzar la concreción del plan delictual. Ciertamente, la generalidad de la primera fórmula, en cuanto alude a un ingreso ilegítimo, torna sobreabundante la referencia a la violación de sistemas de confidencialidad y seguridad de datos, y más aún, cuando posteriormente se establece que el acceso puede concretarse "de cualquier forma". Por ello, la técnica legislativa luce deficiente, debiendo tratarse, en definitiva, de un acceso sin autorización del titular o de la ley.

Debe tenerse presente que la Ley de *Hábeas Data,* en su art. 9, obliga al responsable o usuario de un archivo de datos a adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, prohibiendo la registración de éstos en bancos que no reúnan condiciones técnicas de integridad y seguridad. El objeto de protección penal son los archivos de datos personales, o sea, el conjunto organizado de datos personales que sean objeto de tratamiento o procesamiento electrónico o no, cualquiera fuere la modalidad de su formación, almacenamiento, organización o acceso (art. 2, ley 25.326). Técnicamente, un archivo, registro, base o banco de datos es "un conjunto no redundante de datos organizados e interrelacionados de acuerdo con ciertos atributos comunes en función de los po-

sibles requerimientos de distinta aplicación",[75] que por mandato legal debe estar destinado a dar informes (art. 1, ley 25.326).

Compartimos que desde el punto de vista subjetivo, no sólo el autor debe saber lo que hace —a sabiendas—, sino que debe conocer que accede en forma ilegítima, sin autorización legal o consentimiento del titular de la información personal. Por ello, "… se está castigando un actuar doloso solo compatible con el denominado dolo directo, excluyéndose de tal modo el dolo eventual".[76] Si bien es admisible la tentativa, no debe olvidarse que, tal como acontece con la conducta descrita en el art. 153 *bis* del Código Penal, estamos ante la criminalización de un acto preparatorio punible por una decisión de política criminal.

Se discute si se trata de un delito de acción pública o privada; sin embargo, el segundo incido del art. 73 del Código Penal prevé que la violación de secretos, a excepción de los casos de los arts. 154 y 157, son delitos de acción privada, por lo que, más allá de la tesis del olvido legislativo y de la opinión de parte de la doctrina,[77] una interpretación contraria a la norma, vulneraría el principio de legalidad en perjuicio del eventual inculpado.

La descripción típica se diferencia del art. 153 *bis*, en función de que estas disposiciones poseen un objeto de protección distinto: en este caso, la conducta debe dirigirse contra un banco de datos personales; mientras que en aquel supuesto, el objeto de protección es un sistema o dato informático de acceso restringido.

Por su parte, el inc. 2 prevé la imposición de pena prisión a quién "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".

Esta figura no presenta mayores novedades, pues estamos en presencia de una modalidad especial del convencional delito violación de secretos

(75) Cesario, Roberto, *Hábeas Data. Ley 25.326*, Bs. As., Universidad, 2001, p. 27.

(76) Tazza, Alejandro y Carreras, Eduardo, "La protección del banco de datos personales y otros objetos de tutela penal", Bs. As., La Ley 2008-E, p. 869.

(77) Tazza, y Carreras, *Ibid.*

(arts. 156 y 157 CP), generada por los avances tecnológicos. La Ley de Protección de Datos Personales coloca en cabeza del titular de una base de datos y de todas aquellas personas que intervengan en cualquier fase del tratamiento de la información, la obligación de guardar el secreto profesional, inclusive aún después de finalizada la relación laboral (art. 10, ley 25.326). Asimismo, la obligación de guardar secreto o preservar la confidencialidad de la información, está prevista en leyes específicas (por ejemplo: leyes 11.683, 21.526, 24.766, y otras).

El delito es doloso (admite la modalidad eventual), resultando posible la tentativa.

El obligado al secreto sólo podrá revelarlo, sin incurrir en delito, previa autorización judicial, o ante la existencia de razones fundadas en motivos de seguridad pública, defensa nacional o salud pública.

A su vez, el inc. 3 reprime a quién "ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales". Esta conducta, se encontraba prevista en el inc. 1 del art. 117 *bis* del Código Penal —derogado por la ley 26.388—, dentro de los delitos que afectan el honor de las personas. Por esta razón, la figura derogada sancionaba la inserción de **datos falsos**; en cambio, la redacción actual sólo requiere que el autor inserte o haga insertar **datos** en un archivo de datos personales. No obstante, creemos que la simple conducta de insertar cualquier dato no es suficiente para configurar el injusto penal, se requiere que éste tenga virtualidad suficiente para producir la lesión del bien jurídico. Tazza y Carreras expresan que "la información que se inserta en tales registros puede ser verdadera o falsa, y en este último caso —de ser falsa—, la misma conducta podría configurar, a la vez, el delito de falsedad documental ideológica (arts. 77 y 293 del CP) cuando se trata de instrumento público, o el de injurias o calumnias (arts. 109 y 110 del CP), cuando ello pudiera afectar el honor del perjudicado";[78] sin embargo, la fórmula del art. 77 sólo parece aceptar la existencia de instrumentos privados digitales, excluyendo a los efectos de la ley penal la posibilidad de documentos digitales de naturaleza pública.

Para traer aún más confusión en torno al carácter público o privado de la acción penal que deriva de la comisión de este delito, es interesante

(78) Tazza, Alejandro y Carreras, Eduardo, *op. cit.*

señalar que en su versión anterior (ver el texto del art. 117 *bis*) era de acción pública.

Por último, en cualquiera de los tres supuestos, cuando el autor sea funcionario público (art. 77 CP) sufrirá también pena de inhabilitación especial de uno a cuatro años.

6 | Consideraciones preliminares sobre el Anteproyecto de Código Penal de la Nación (decreto 678/2012)

En primer término, se propone un cambio de rúbrica al capítulo correspondiente del catálogo punitivo, reemplazando el de "violación de secretos y de la privacidad" por el de "violación de comunicaciones y de la privacidad", pese a que se encuentran incluidas entre estas disposiciones aquellas referidas al secreto profesional y funcional.

Las conductas actualmente previstas en el art. 153 del CP son ordenadas en el art. 119 (violación de comunicaciones) y se aumentan los montos punitivos, previéndose la pena de prisión de seis meses a dos años y multa de diez a ciento cincuenta días. Si bien el artículo prevé la pena de multa en forma conjunta atento usar la conjunción "y", debe tenerse en cuenta la alternativa prevista para supuestos de escasa lesividad o significancia jurídico penal consiste en la imposición alternativa de una multa reparatoria o la determinación de una pena judicial por debajo del mínimo legal (arts. 3 inc. a y 22 inc. g).

Las conductas típicas en términos generales se mantiene inalterables, pero son organizadas en cuatro incisos, correspondiendo destacar que se incluye expresamente a las comunicaciones telefónicas y se reemplaza la voz "u otro papel privado" por "un papel privado", lo que nos parece de mejor técnica legislativa, atento las razones enunciadas al analizar ut supra el art. 153 del CP. Asimismo, en el inc. d) se mantiene la expresión "cualquier sistema de carácter privado o acceso restringido", respecto de la cual ya hemos señalado que no se aprecian con facilidad las diferencias

existentes entre sistemas privados o de acceso restringido, y en todo caso, ello seguirá dando lugar a distintas interpretaciones. No obstante, es claro que la norma no sería de aplicación si el sistema es abierto, accesible a una generalidad de individuos.

A su vez, las agravantes de la figura básica están previstas en el inc. 2 del art. 120 del Anteproyecto. Se mantiene el incremento punitivo cuando la conducta es ejecutada por un funcionario público abusando de su condición e incorpora también el abuso de oficio o profesión del agente, aun cuando no se tratare de un funcionario público.

El citado art. 120 proyecta en su inc. 1 la siguiente figura delictiva: "Será reprimido con prisión de seis (6) meses a dos (2) años y multa de diez a ciento cincuenta días, el que vulnerare la privacidad de otro, mediante la utilización de artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o imagen, o se hiciere de registros no destinados a la publicidad". Con esta inclusión se propone subsanar la omisión en la que incurrió la Ley de Delitos Informáticos. Recordemos que la ley 26.388 no reguló el uso de las cámaras ocultas, frecuentemente utilizadas en investigaciones periodísticas, con el argumento de que era posible afectar la libertad de expresión, y optó por postergar su tratamiento.[79] El texto del Anteproyecto es similar al del fallido art. 153 *ter* del Código Penal: "Será reprimido con prisión de un mes a dos años, el que ilegítimamente y para vulnerar la privacidad de otro, utilizando mecanismos de escucha, intercepción, transmisión, grabación o reproducción de voces, sonidos o imágenes, obtuviere, difundiere, revelare o cediere a terceros los datos o hechos descubiertos o las imágenes captadas".

En los arts. 119 y 120 si bien se agrava la pena cuando interviene un funcionario público abusando de su condición, no se prevé en forma conjunta la pena de inhabilitación. En ambos casos, sí se prevé la pena conjunta de multa y se agrava la pena de prisión con un mínimo de un año y un máximo de cuatro.

En el art. 121 del Anteproyecto se castiga la comunicación o publicación indebida de los instrumentos, registros o contenidos a los que se refieren los artículos precedentes —a saber: una comunicación electrónica,

(79) Cámara de Diputados de la Nación, OD Nº 1227, 26/10/2006.

telefónica, una carta, un pliego cerrado, un papel privado, un despacho telegráfico o telefónico o de otra naturaleza o registros obtenidos mediante la utilización de artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o imagen—. En el inc. 1 se reprime con prisión de seis meses a tres años, multa de diez a ciento cincuenta días e inhabilitación de uno a cuatro años, al que hallándose en posesión de estos instrumentos, registros o contenidos, los comunicare, publicare o los hiciere publicar, indebidamente. De seguido, el inc. 2 prevé igual pena para quien los hiciere publicar, siempre que no estuvieren destinados a la publicidad —aunque le fueren dirigidos— si el hecho causare o pudiere causar perjuicios. En la parte Exposición de Motivos se aclara que en este inciso se pune la conducta de quien posee el objeto de protección penal "debidamente", por lo que entendemos que el injusto radica en el hecho darlo a conocer a un número indeterminado de personas —aunque le estuviere dirigido— cuando su destino no era la publicidad y con ello se pueda causar un perjuicio (daño potencial). A *contrario sensu* puede afirmarse entonces que la conducta prevista en el primer inciso de la norma abarca aquellos supuestos en los que el autor ha entrado en posesión del material en forma indebida a través de cualquiera de las formas enunciadas en los arts. 119 y 120 del Anteproyecto.[80] Sin embargo, por su ubicación y función gramatical el adverbio "indebidamente" se halla vinculado a los verbos típicos y no a la posesión previa de los materiales, por lo que sería recomendable dotar de mayor claridad a la fórmula legal propuesta. Finalmente, la norma proyectada exime de responsabilidad penal a quien hubiere obrado con el propósito inequívoco de proteger un interés público actual. En síntesis, se ordenan bajo una misma disposición legal las conductas que actualmente se encuentran previstas en los arts. 153, 3 párr. y 155 del CP, lo cual nos parece de buena técnica legislativa.

Se suprime el art. 154 del CP y en el art. 122 del Anteproyecto se reproducen en dos incisos los vigentes arts. 156 y 157, ocupándose en forma conjunta del secreto profesional y funcional. Como dato relevante, en este caso se prevé la pena de multa en forma alternativa utilizando la conjunción disyuntiva "o". Asimismo, en la Exposición de Motivos se aclara que si bien con mayor frecuencia el sujeto pasivo del secreto funcional es la Administración o el Estado, ello no es una regla, "pues

(80) Al igual que en el art. 153 del CP, donde se utiliza la fórmula "si el autor además comunicare a otro o publicare...".

la conducta tipificada —al menos en buen número de casos— resulta pluriofensiva: el funcionario que revela los datos de la ficha de salud de una persona reservada en una oficina de personal, no sólo lesiona a la administración".

Finalmente, en el art. 123 se prevé el delito de "acceso ilegítimo a información". En el inc. 1° se reproduce el texto del art. 153 *bis* del CP, se elimina la mención expresa al carácter subsidiario de la figura y se sustituye la pena de prisión por la de multa de diez a cien días. La previsión de una pena más benigna responde al reclamo de un importante sector de la doctrina que entiende que esta conducta, como antesala de delitos más graves (por ejemplo: otros atentados contra la intimidad, sabotaje, espionaje o defraudaciones), no posee relevancia penal o debe ser considerada una contravención.[81] Si bien se mantuvo el carácter de delito se suprimió como dijimos la pena privativa de libertad. El acceso —al igual que en el actual art. 153 *bis* del catálogo punitivo— puede ser a un "sistema" o a un "dato" informático, lo cual entendemos nos es superfluo. Veamos, si la acción del denominado *hacker* simple consiste en acceder a un sistema informático, sin que dicho acceso importe al mismo tiempo conocer datos informáticos de carácter confidencial o privado, nos parece que la conducta no posee relevancia penal o, en todo caso, la misma sería mínima. Por ello, la sustitución de la pena de prisión por la de multa con un mínimo de diez días nos parece adecuada. Ahora bien, si el autor mediante el acceso ilegítimo a datos informáticos obtuvo información confidencial o privada —que no constituya, a su vez, una comunicación electrónica o un registro obtenido a través de artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o imagen, lo que podría ser abarcado por otras disposiciones— se advierte cierta desproporción con las penas previstas para los delitos de "violación de comunicaciones" y "violación de la privacidad" (arts. 119 y 120 del Anteproyecto), pues ante similar afectación del bien jurídico se prevé una reacción estatal de distinta entidad.

(81) En este sentido José Saez Capel y Claudia Velciov sostienen que: "... tales conductas carecen de entidad suficiente para merecer la intervención del Derecho penal; o bien se materializan en otro hecho más grave, o caso contrario, resultan inofensivas, y su incriminación atenta contra el principio de lesividad e intervención mínima..."(Saez Capel, José y Velciov, Claudia, "Artículo 153 bis", en Eugenio Zaffaroni y David Baigún (dirs.), *Código Penal y normas complementarias. Análisis doctrinal y jurisprudencial*, Bs. As., Hammurabi, 2008, tomo V, p. 743).

Por su parte, en el inc. 2 se prevé una pena de prisión de seis meses a dos años para los mismos casos descriptos en el segundo párrafo del actual art. 153 *bis* del CP, incorporándose al tipo penal la mención de los servicios de salud.[82] Finalmente, como novedad, si el hecho se cometiere con el fin de obtener información sensible a la defensa nacional, se proyecta elevar el máximo de la pena de prisión a cuatro años.

Los tres primeros apartados del inciso tercero del art. 123 del Anteproyecto reproducen en términos generales los tres incisos del art. 157 *bis* del CP, proponiendo algunas modificaciones a la redacción típica que redundan en una mejor técnica legislativa. Se suprimen en los delitos de acceso no autorizado a un banco de datos personales y revelación de información registrada en un banco de datos personales el adverbio "ilegítimamente", que fuera criticado por toda la doctrina por sobreabundante. Asimismo se simplifica y clarifica la descripción de la conducta prevista actualmente en el inc. 1 del art. 157 *bis* del CP a través de la siguiente fórmula: "será penado (...) el que a sabiendas y violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales".[83] El apartado d) se complementa con el apartado a), sancionando la obtención de datos personales, financieros o confidenciales mediante cualquier ardid o engaño, por lo que se requiere que el sujeto pasivo sea una persona física.

En lo referente a los apartados e) y f), dado su carácter novedoso, es importante transcribir las consideraciones efectuadas en la Exposición de Motivos:

> "El apartado e) tipifica la conducta no sólo de quien provea los instrumentos para la comisión de los delitos previamente tipificados, sino que se incluye también su tenencia cuando sean inequívocamente destinados a su comisión. Se trata de a tipificación de un acto preparatorio, como el tradicional referido a la falsificación. Si el hecho se tentare, esta tipicidad desaparece en función de las reglas del concurso aparente. El apart. f) pro-

(82) Compartimos con Saez Capel y Velciov que debería establecerse con precisión el alcance del concepto "servicio público" (Saez Capel, y Velciov, *op. cit.*, p. 747).

(83) Ver las críticas efectuadas en forma precedente al art. 157 ***bis*** del CP.

> puesto, tipifica una conducta frecuente y altamente peligrosa en la comunicación. Si bien no está referida a datos personales, se trata de una grave suposición de identidad, perjudicial para el buen nombre del real portador del nombre y con capacidad para producir serios daños".

En el primer caso basta con la tenencia de los materiales siempre y cuando surja en forma inequívoca su finalidad ilícita. Es decir, estamos frente a un delito de peligro abstracto, no obstante lo cual, entendemos se requiere establecer una vinculación entre el bien jurídico y la acción del autor, pues la descripción típica no puede ser concebida como un delito formal. En otras palabras, es necesario que la conducta resulte riesgosa aunque no se traduzca en un peligro concreto. En consecuencia, en nuestra opinión, si por algún motivo los artificios técnicos resultan absolutamente inidóneos para el fin para el cual fueron concebidos no puede considerarse típica su tenencia. La utilización del término "inequívocamente" es correcta en este caso —a diferencia de lo que sucede en el segundo párr. del art. 14 de la ley 23.737—,[(84)] ya que la carga de la prueba recae en la parte acusadora.

En el segundo supuesto, se propone legislar el delito de usurpación de identidad, respondiendo a un reclamo social. En este sentido, cabe mencionar que en nuestro país se creó un Centro de Asistencia a las Víctimas de Robo de Identidad, y además, la Dirección Nacional de Protección de Datos Personales dispuso la creación de un Registro de Víctimas de Robo de Identidad. Por otro lado, y más allá de su acierto o no a la luz de los principios de *ultima ratio* y carácter subsidiario del derecho penal, existían otras iniciativas legislativas para tipificar el robo de identidad digital, como el proyecto de la diputada Natalia Gambaro, quién propició la incorporación al Código Penal del art. 139 *ter:*

> "Será reprimido con prisión de 6 meses a 3 años el que adoptare, creare, apropiare o utilizare, a través de Internet, cualquier sistema informático, o medio de comunicación, la identidad de una persona física o jurídica que no le pertenezca. La pena será de 2 a 6 años de prisión cuando el autor asumiera la identidad

(84) Véase el fallo de la CSJN, "Vega Giménez, Claudio Esteban s/ Tenencia Simple de Estupefacientes", V. 1283, causa N° 660, 27/12/2006.

de un menor de edad o tuviese contacto con una persona menor de dieciséis años, aunque mediare su consentimiento o sea funcionario público en ejercicio de sus funciones".

Afortunadamente, en el Anteproyecto se requiere que el agente actúe con el propósito de causar un perjuicio.

Mención aparte, consideramos que esta última conducta podría haber sido incluidas en el mismo artículo como inc. 4 ya que no guarda relación con el art. 157 *bis* del Código sustantivo.

Finalmente, el inc. 4, cuando el sujeto activo fuere funcionario público, repite la fórmula prevista en el último párrafo del art. 157 *bis*, mantiene la pena conjunta de inhabilitación, pero aumenta su máximo a cinco años.

7 | Palabras finales

Hemos visto a lo largo de este trabajo las dificultades y desafíos que presenta la protección de la privacidad en la "sociedad de la información", en la que los recursos técnicos reducen cada vez más la posibilidad real de que los individuos gocen de un ámbito de dominio exclusivo, donde se encuentren solos, exentos de la injerencia arbitraria o ilegal de terceros o del Estado. De esta manera, somos testigos de una importante transformación, fáctica y cultural, del bien jurídico, que el derecho necesariamente debe contemplar y regular. En este contexto, resultó razonable la sanción de la ley 26.388 de Delitos Informáticos, y más aún, su inclusión en el catálogo punitivo, evitando así la proliferación de leyes especiales que conducen inexorablemente a la ruptura del sistema de código.

No obstante, creemos corresponde ser cautos a la hora de generar expectativas en punto a la efectiva protección del bien jurídico a través del derecho penal en materia de delitos cometidos mediante el uso de las nuevas tecnologías, por cuanto la herramienta punitiva no sólo actúa cuando la lesión material se ha concretado, sino que en esta temática específica surge en forma particularmente manifiesta la mayor idoneidad de las medidas extra-penales, principalmente sustentadas en el suministro de información al usuario como política pública sobre el uso seguro y responsable de estos dispositivos electrónicos.

Asimismo, nos hemos ocupado del estudio dogmático de los "delitos informáticos" contemplados en nuestro Código Penal, a fin de exponer nuestro punto de vista sobre los alcances y requisitos típicos de estas figuras penales en el marco de un Estado de Derecho, siempre desde una hermenéutica reductora del poder punitivo.

Por último, hemos realizado un análisis preliminar del Anteproyecto de Código Penal de la Nación elaborado por la comisión *ad hoc* encabezada por el Dr. Raúl E. Zaffaroni, e integrada por los Dres. León Arslanian, Ricardo Gil Lavedra, María Elena Barbagelata y Federico Pinedo,[85] el que, como bien se ha dicho, constituye "...un plan admirable que tiene las mejores cartas para lograr (re)construir un Código Penal que resulte adecuado al modelo liberal y humanista impuesto en la materia por los textos políticos fundamentales de nuestro Estado constitucional y democrático de derecho", que implica la continuidad de la reforma penal emprendida en 2004 y que debiera extenderse al régimen procesal penal.[86]

(85) Comisión para la Elaboración del Proyecto de Ley de Reforma, Actualización e Integración del Código Penal de la Nación (Decreto 678/12).

(86) Pastor, Daniel R., "La recodificación penal en marcha. Una iniciativa ideal para la racionalización legislativa", en *Revista Pensar en Derecho*, Bs. As., Eudeba, 2012, p. 37.

Convenio sobre Cibercriminalidad de Budapest y el Mercosur

Propuestas de derecho penal material y su armonización con la legislación regional sudamericana

por **MARCELO A. RIQUERT**[1]

I | Introducción

Luego de que, en noviembre de 1996, el **Comité europeo sobre problemas penales** creó un comité de expertos para trabajar el fenómeno de la delincuencia asociada a la tecnología; el Consejo de Europa impulsó y abrió a la firma el conocido **Convenio sobre Cibercriminalidad**,[2] en su reunión celebrada en la ciudad de Budapest el 23 de noviembre de 2001. Dicho Convenio está en vigor desde el 1° de julio de 2004, con un proto-

(1) Profesor de Derecho Penal, Facultad de Derecho de la Universidad Nacional de Mar del Plata. Presidente (2013-2015) de la Asociación Argentina de Profesores de Derecho Penal (AAPDP).

(2) Ver Morales García, "Apuntes de política criminal en el contexto tecnológico. Una aproximación a la Convención del Consejo de Europa sobre Cyber-crime", en AAVV *"Delincuencia Informática. Problemas de responsabilidad"*, Madrid, Cuadernos de Derecho Judicial IX-2002, Consejo General del Poder Judicial 2002, p. 17. No obstante, algunos prefieren situar el germen del convenio aún más atrás, en 1983, cuando una reunión de expertos recomendó a la OCDE (Organización para la Cooperación y Desarrollo Económico) la necesidad de

colo adicional del 28 de enero de 2003 sobre la lucha contra el racismo y la xenofobia por Internet.

Para Óscar Morales García, fue el proyecto legislativo más ambicioso en la materia. Además, afirma que, por atemperar algunas de sus propuestas originales durante la revisión de los borradores, ha terminado plasmando "en una Convención político criminalmente aceptable".(3)

Justamente por la búsqueda de consensos entre los Estados que participaron en su confección, Rovira del Canto dijo que se trataba de una "Convención de mínimos".(4) Si bien es una iniciativa de la Unión Europea, ha sido firmado por numerosos países extracomunitarios, como Estados Unidos o Japón. Argentina adhirió en 2010.(5) Además, dentro del margen latinoamericano, se encuentran Costa Rica, República Dominicana, México y Chile.

Esta nota comparte la concepción sobre el Consejo de Europa hecha por Walter Perron en tanto organización de derecho internacional que, claramente, tiene un alcance que va más allá de los Estados miembros de la Unión Europea, cuyo núcleo está expuesto en la Convención Europea sobre derechos humanos. El Consejo no tiene facultades soberanas propias, sino que su objeto es influir en el desarrollo de los Estados miembros a través de recomendaciones y tratados. Su instrumento más importante es el Tribunal Europeo de Derechos Humanos (TEDH), cuya jurisprudencia es de superlativa importancia y ante el que todo ciudadano de un estado

armonización en los delitos informáticos. Ésto materializó tres años después, punto en que el Consejo de Europa tomó la iniciativa y publicó en 1989 la Recomendación n° 89, mostrando la tendencia que desembocó en Budapest (Ver: Díaz Gómez, Andrés, "El delito informático, su problemática y la cooperación internacional como paradigma de su solución: el Convenio de Budapest", en *Revista Electrónica de Derecho* de la *Universidad de La Rioja* (REDUR), n° 8, diciembre de 2010, p. 195.

(3) Morales García, *op. cit.*, p. 16.

(4) Rovira del Canto, Enrique, "Ciberdelincuencia intrusiva: hawking y grooming", conferencia brindada en Barcelona, noviembre de 2010, p. 4., [en línea] http://www.iaitg.eu/media-pool/67/671026/data/Ciberdelincuencia_intrusiva_hacking_y_grooming_Enrique_Rovira.pdf

(5) En el marco de la Conferencia de Estrasburgo sobre Cibercrimen, celebrada en marzo de 2010, lo que hace —como bien resalta Cherñavsky— que se realicen las reformas pertinentes para ratificar la Convención (Cherñavsky, Nora, "El delito informático", en De Luca, Javier A. (coord.), *XI Encuentro de Profesores de Derecho Penal de la República Argentina*, Buenos Aires, La Ley/UBA/AAPDP, 2013 (en prensa), p. 288.

miembro puede comparecer en el marco de una petición individual. El nombrado individualiza precisamente como el segundo sector más importante las numerosas convenciones respecto de distintos aspectos del derecho penal y procesal penal; tales como las relativas a extradición, asistencia jurídica recíproca, lucha contra el terrorismo o un variado conjunto de delitos conglobados bajo la designación de "criminalidad organizada" —lavado, tráfico de drogas, financiamiento del terrorismo— y otros que sólo pueden ser protegidos a nivel transnacional —corrupción pública y privada, protección del medio ambiente, tráfico ilegal de personas, explotación sexual de niños, *insider trading,* manipulaciones del mercado y delitos informáticos—.[6]

Por eso, en un trabajo previo,[7] señalé que el citado Convenio se ha constituido en una referencia insoslayable en términos de armonización legislativa en la materia[8] y que la normativa argentina no tiene al presente mayor problema de compatibilidad con los estándares mínimos que aquél reclama en lo referente al derecho penal sustancial. Mientras que en lo adjetivo o formal es donde puede advertirse algún déficit de mayor significación.[9] No se trata de un problema exclusivo de nuestro país, sino que, como bien advierte Marcos Salt, se trata de un rasgo extendido en toda la legislación latinoamericana. Pues sus previsiones procesales han sido

(6) Perron Walter, "Perspectivas de la unificación del derecho penal y del derecho procesal en el marco de la Unión Europea", en AAVV, *Estudios sobre Justicia Penal. Homenaje al Profesor Julio B. J. Maier*, Bs. As., Editores del Puerto, 2005, pp. 734/735 y 737/738.

(7) Riquert, Marcelo, "Delincuencia informática y control social: ¿excusa y consecuencia?", en *Revista Jurídica Facultad de Derecho de la UNMDP,* n° 6, 2011, pp. 67/99; y [en línea] http://perso.unifr.ch/derechopenal/assets/files/articulos/a_20120208_01.pdf

(8) Se trataría de uno de esos casos puntuales en que se provoca una cierta unificación por una "necesidad práctica" en un "ámbito parcial" del derecho penal, conforme la terminología de Hans Joachim Hirsch, quien no se muestra particularmente favorable hacia un posible avance en pos de una unificación general del derecho penal europeo (ver Hirsh, Hans Joachim, "Cuestiones acerca de la armonización del derecho penal y procesal penal en la Unión Europea", en AAVV, *Estudios sobre..., op. cit.,* p. 668.

(9) El convenio prevé reglas relativas al ámbito de aplicación (art. 14), condiciones y garantías (art. 15), competencia, conservación inmediata de datos, preservación de datos incluidos los de tráfico (art. 16), registro y decomiso de datos informáticos almacenados (Título 4 de la Sección 2°), recogida en tiempo real de datos informáticos y datos de tráfico (art. 20), interceptación de datos relativos al contenido (art. 21), cooperación (cuyos principios generales enuncia el art. 23), colaboración y asistencia internacionales en investigación (art. 31) y medidas cautelares (art. 29; incluyendo en su art. 35 la llamada "Red 24x7", es decir, constituir un punto de contacto las 24 horas del día, los 7 días de la semana) o a la extradición (art. 24).

diseñadas pensando en la evidencia física y no en la digital. En muchos casos los problemas que se presentan terminan siendo solucionados por vía jurisprudencial aplicando analógicamente criterios y reglas de las pruebas físicas. El retraso en la adopción de reformas procesales respecto de las modificaciones en el derecho penal material se verifica también en otras regiones —Alemania, Portugal y España—.[10]

La situación de nuestra región es curiosa. Con la adopción de modernos códigos de corte acusatorio, se ha producido una masiva transformación de los sistemas procesales en los últimos quince años. Sin embargo, ha dejado sin mayores variaciones los s dedicados a la prueba, que permanecen con una semejanza notable a los de los viejos digestos inquisitivos o mixtos.

Hecha la aclaración recuerdo que, para fundar la necesidad de provocar aquella armonización, desde hace tiempo se hace hincapié en que las fronteras nacionales constituyen un obstáculo evidente para la detección, investigación, persecución y castigo de los autores de los delitos perpetrados mediante el uso de las nuevas tecnologías de la información y comunicación (TIC). En cambio, Internet está configurada como un espacio sin fronteras para aquéllos. Hay una ineludible dimensión supranacional[11] y, para afrontarla, es claro que la vía más conveniente no es la antigua cooperación bilateral; sino el impulso de esfuerzos de armonización regional mediante convenios multilaterales, como el que ahora nos ocupa.[12] Además, como resalta Lezertua, la armonización sustantiva es un elemento indispensable pero no suficiente para llevar a cabo un combate eficaz

(10) Ver Salt, Marcos, *Criminal procedure law provisions on cybercrime in Latin American regarding their compliance with the Budapest Convention (Argentina, Chile, Colombia, Costa Rica, México, Paraguay and Perú)*, Estrasburgo, council of Europe, 12 de abril de 2011, p. 4.

(11) En este sentido, parece importante no perder de vista que, en el caso de nuestro objeto de atención aquí, estamos en general frente a lo que constituiría en su evolución un "derecho penal transnacional". Es decir, referido a crímenes transnacionales. Y no un "derecho penal internacional" stricto sensu, referido a crímenes internacionales como los reconocidos por el Estatuto de Roma. A saber: genocidio, crímenes de lesa humanidad, de guerra y el crimen de agresión (Romeo Malanda, Sergio, "Un nuevo modelo de derecho penal transnacional: el derecho penal de la Unión Europea tras el Tratado de Lisboa", en *Estudios Penales y Criminológicos*, Servicio de Publicaciones de la Universidad de Santiago de Compostela, vol. XXXII, 2012, p. 318. El autor, aquí, alude a las opiniones de autores como Boister y Sieber).

(12) Díaz Gómez, *op. cit.*, p. 183.

contra la ciberdelincuencia. Debe ser acompañada de otro relativo a los instrumentos apropiados para detectar, investigar, procesar y castigar a los autores de esas infracciones.(13)

Jansky y Lombaert destacan que la Comisión Europea, en su comunicación "Hacia una estrategia general en la lucha contra la ciberdelincuencia", distingue una tercer área de actividades principales en la elaboración de una estrategia europea coherente para luchar contra la ciberdelincuencia en cooperación con los Estados miembros de la Unión Europea; tanto con las instituciones de la región como las internacionales. Señalan, además, que la legislación y la ejecución de la ley a nivel transfronterizo debe articularse con la colaboración de los sectores público y privado.(14) Cherñavsky ha destacado la experiencia adquirida por Europol en la coordinación de programas sobre cibercrimen, de respuestas y estrategias, incluso respecto de la lucha contra el terrorismo. A su vez destacó la necesidad de que Argentina desarrolle esa experticia en cooperación internacional y con el intercambio de información tanto contra del cibercrimen como de los delitos financieros, del lavado de dinero y del terrorismo.(15)

En el presente trabajo, sólo será objeto de tratamiento lo concerniente al derecho penal material. Queda, entonces, para una futura oportunidad lo vinculado a aspectos procesales y operativos.

En un estudio comparativo de derecho regional anterior cotejé la situación argentina con los restantes países miembros plenos del Mercosur,(16) par-

(13) Manuel Lezertua, "El proyecto de Convenio sobre el Cybercrimen del Consejo de Europa", en López Ortega, Juan José (dir.), *Internet y Derecho Penal*, Madrid, *Cuadernos de Derecho Judicial* X-2001, Consejo General del Poder Judicial, 2001, p. 25.

(14) Radomir Jansky y Ruben Lombaert, "Hacia una estrategia europea unificada para combatir la ciberdelincuencia", en *E) NAC. E-newsletter. En la lucha contra el cibercrimen*, nº 4, octubre de 2009, p. 39.

(15) Cherñavsky, *op. cit.*, p. 288. Díaz Gómez sugiere que la cooperación internacional —que liga a la constitución de un derecho procesal penal internacional— resultaría el paradigma de la solución a la problemática de la ciberdelincuencia (*op. cit.*, p. 187), aunque más adelante en su trabajo rescata la dimensión de armonización en materia sustantiva, que constituiría un derecho penal internacional (*ibid.*, p. 191).

(16) Riquert, Marcelo, *Delincuencia informática en la Argentina y el Mercosur*, Bs. As., EDIAR, 2009, prologada por el Prof. Emérito de la UBA, Dr. David Baigún. Ver, en particular, el capítulo VII. Téngase presente, además, que en ese momento los miembros plenos eran sólo

tiendo de nuestra regulación nacional. En cambio, en éste, la tarea no sólo comprende una base mayor de países comparados —se incorporan los estados asociados—,[17] sino que se concreta tomando como eje el articulado que propone Budapest en su capítulo II —"Medidas que deben ser adoptadas a nivel nacional"—, cuya sección 1 se dedica al "Derecho penal material" (arts. 2 a 13) y se subdivide en cinco títulos.

La situación de nuestro bloque regional —más allá de su ampliación,[18] en cuanto se lo relaciona con el de origen del instrumento internacional citado, la Unión Europea,— no ha sufrido cambios.

Con buena voluntad, del Mercosur puede decirse que se mantiene en el estadio correspondiente al momento previo al fundacional Tratado de Maastricht —año 1992—, cuando desde la estructura comunitaria no había competencia alguna en el ámbito del derecho penal y procesal penal aunque, como resalta Walter Perron:

> "ya entonces se era consciente de que, debido a los múltiples problemas provocados por la criminalidad transnacional e internacional, que afectaba bienes jurídicos regionales, se había tor-

la República Argentina, la República Federativa de Brasil, la República del Paraguay y la República Oriental del Uruguay. Estaba en trámite de acceder a tal condición la República Bolivariana de Venezuela, al presente finalizado. Se encuentra en vías de adquirir la calidad plena el Estado Plurinacional de Bolivia.

(17) Estos son en la actualidad Chile, Colombia, Ecuador y Perú. Aún están en trámite de asociación Guyana y Surinam, por lo que no forman parte de la base comparada.

(18) Vale aclarar que esta afirmación se corresponde estrictamente con la cuestión penal ya que, como señalan Piccone y Mangini, hoy se habla de la aparición de un nuevo paradigma en el regionalismo sudamericano —cuya expresión más acabada sería la UNASUR—, definido como "post-comercial" (Celli, Salles, Tussie y Peixoto), "post-liberal" (Motta Veiga y Ríos), "post-neoliberal" o "post-hegemónico" (Serbin). Sus elementos distintivos serían: a) la revalorización de la agenda política frente a la agenda económico-comercial; b) la adopción de una nueva agenda de desarrollo, distanciándose de las estrategias de liberalización comercial del "regionalismo abierto"; c) el despliegue de una agenda positiva de integración orientada a una mayor coordinación político-estratégica y el desarrollo de una institucionalidad común en áreas no comerciales, como paz y seguridad regional (Piccone, V.; Mangini, M., "UNASUR en el contexto del regionalismo y los paradigmas de la integración latinoamericana", en *Revista Derecho Público*, año II, nº 5, Buenos Aires, Ediciones Infojus, pp. 196/197). Al presente hay una simetría en la conformación del Mercosur y la Unasur. Ya que todos los miembros y asociados del primero integran la segunda y Guyana y Surinam, que integran la segunda, ya se ha señalado que han solicitado ser considerados estados asociados al primero.

> nado necesaria una colaboración más estrecha entre los países, así como una armonización del derecho penal".[19]

Debe tenerse presente que en el Convenio no se proporciona una definición general de "delito informático", "ciberdelito" o de "cibercrimen". Por lo que podría decirse que, frente al dilema en la teoría criminológica, ante las nuevas formas de delito generadas por las TIC —sintetizado por Zavrsnik como los enfoques "vino viejo, botella nueva" (Grabosky) y "vino nuevo sin botella" (Wall)—,[20] no ha tomado partido.

En los cuatro primeros títulos se enumera una serie de comportamientos —en total nueve, que contienen una o varias conductas, siempre "intencionales" para la tradición anglosajona, o "dolosas" para el modelo dogmático europeo-continental— a la que los estados son exhortados a considerar como infracciones penales en su legislación interna.

No se trata, entonces, de la provisión de una **redacción tipo** de delitos, cual suerte de receta inalterable; sino de una formulación genérica, abierta y, en algunos casos, con alternativas que los signatarios puedan adaptar conforme a su propio diseño de derecho local. Esta característica, lógica y apropiada para una suerte de convenio-marco, dificulta el cotejo con la normativa nacional; ya que dentro del universo de casos en consideración hay legislación pre-convenio y post-convenio de países que lo han firmado y otros que no, que han realizado una tipificación más amplia o más restrictiva y, a la vez, que lo hicieron en forma más concentrada o más dispersa en un doble sentido:

a. en cuanto a la adopción de una ley especial o un capítulo específico en su Código Penal, o en alternadas modificaciones en leyes especiales y el propio Código, o difuminada o sectorizada dentro del último;

(19) Perrón, *op. cit.*, p. 729. Con "Maasricht", el derecho europeo comunitario hasta entonces existente configuró la denominada "primera columna", lo relativo a política exterior y seguridad común de todos los estados miembros pasó a ser la "segunda columna" y, finalmente, la "tercera columna" se conformó con lo relativo a la cooperación interestatal en los ámbitos de Interior y Justicia lo que, como destaca Perron, no implicaba la creación de un nuevo derecho supranacional pero sí dejaba en claro que la cooperación internacional en materia jurídico-penal resultaba un objeto que hacía al interés común de todos los estados miembros de la Unión Europea (*Ibid.*, p. 730).

(20) Zavrsnik, Ales "La intervención del sistema de justicia penal en las amenazas a la ciberseguridad: ¿panacea o caja de Pandora?", en *E-newsletter,* n° 44, diciembre de 2008, p. 3. Seña-

b. en cuanto el Convenio, brinda en algún artículo una serie de verbos típicos para los que no hay una sola norma nacional que los reciba juntos, sino que puede hacerlo desperdigados entre diferentes tipicidades o, incluso, sólo parcialmente.

Es esencial no perder de vista este factor; porque, al concretar la comparación tendiente a establecer asertiva o negativamente la recepción de una propuesta en el nivel nacional, en ocasiones, se improvisa una respuesta que sería aproximada. Es decir, puede darse el caso de que, sin haber correspondencia precisa, aun con algún déficit menor de tipicidad; no pueda sostenerse la absoluta laguna de punibilidad local y, por eso, se entienda que existe cumplimiento con el requerimiento externo, aunque sea parcial.

Tampoco en el convenio se indica o sugiere en cada caso algún tipo de sanción concreta. En el artículo 13, en forma general, se habla de la respuesta penal de personas físicas y jurídicas. Ésta debe ser efectiva, proporcionada y disuasoria. En el caso de las personas jurídicas, puede tratarse tanto de sanciones penales como civiles o administrativas. Y dentro de las penas, puede incluirse las pecuniarias. En cambio, en caso de las personas físicas, puede incluirse las penas privativas de libertad.

2 | Las infracciones contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos

Se comenzará siguiendo el orden propuesto en el Convenio de Budapest —Título 1 de la Sección 1 del II, dedicado a las "Infracciones contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos"—, donde se indica que los estados tipificarán penalmente las siguientes conductas, agrupadas en cinco artículos: acceso ilícito, interceptación ilícita, atentado contra la integridad de los datos, atentado

la que, en la actualidad, pareciera que ambos enfoques son correctos, o no, pero que los nuevos conceptos sobre información, computadoras y redes han posicionado al segundo en la vanguardia de la investigación criminológica.

contra la integridad del sistema y abuso de equipos e instrumentos técnicos. Antes de pasar al detalle comparativo, se aclara que, luego de la transcripción del texto del convenio, se ha seguido un orden alfabético que no distingue entre miembros plenos y asociados del Mercosur.

2.1 | Acceso ilícito (art. 2)

> "Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, el acceso doloso y sin autorización a todo o parte de un sistema informático. Las Partes podrán exigir que la infracción sea cometida con vulneración de medidas de seguridad, con la intención de obtener los datos informáticos o con otra intención delictiva, o también podrán requerir que la infracción se perpetre en un sistema informático conectado a otro sistema informático".(21)

a. Esta primera figura consagra uno de los supuestos prototípicos de lo que algunos clasifican como "ciberdelincuencia intrusiva". Es decir, aquellos configurados por ataques contra la intimidad y la privacidad que, autores como Rovira del Canto, extienden al honor, la intimidad personal y familiar, la propia imagen, el domicilio, el secreto de las comunicaciones o incluso el uso adecuado y correcto de la informática.(22)

(21) Esta propuesta típica, con algún cambio, fue reafirmada mediante la Decisión Marco 2005/222/JAI del Consejo, de 24 de febrero de 2005, relativa a los ataques contra los sistemas de información, con esta redacción: "Artículo 2°. Acceso ilegal a los sistemas de información. 1) Cada Estado miembro adoptará las medidas necesarias para que el acceso intencionado sin autorización al conjunto o a una parte de un sistema de información sea sancionable como infracción penal, al menos en los casos que no sean de menor gravedad. 2) Cada Estado miembro podrá decidir que las conductas mencionadas en el apartado 1 sean objeto de acciones judiciales únicamente cuando la infracción se cometa transgrediendo medidas de seguridad".
A su vez, ha sido sustituido por el artículo 3° de la Directiva 2013/40/UE del Parlamento Europeo y del Consejo de 12 de agosto de 2013 relativa a los ataques contra los sistemas de información, fusionando ambos párrafos del siguiente modo: "Los Estados miembros adoptarán las medidas necesarias para que, cuando haya sido realizado intencionalmente, el acceso sin autorización al conjunto o a una parte de un sistema de información sea sancionable como infracción penal cuando se haya cometido con violación de una medida de seguridad, al menos en los casos que no sean de menor gravedad".

(22) Rovira del Canto, *op.cit.*, p. 1. Completa su clasificación tripartita con la "ciberdelincuencia económica", con los ataques de contenido patrimonial y el "ciberespionaje y ciberterrorismo", que se refiere a los ataques contra bienes supraindividuales.

Es interesante resaltar que, si bien el Convenio toma partido por considerar delito el simple *hacking,* permite que los signatarios introduzcan condicionantes —la vulneración de medidas de seguridad— y elementos subjetivos distintos del dolo —la intención de obtener datos u otra intención delictiva—. También permite que la tipificación se limite a casos de acceso a sistemas informáticos a los que esté conectado otro. Sin embargo, cuando se observa la recepción nacional, en general, se ha terminado consagrando figuras penales de mayor amplitud sin hacer uso de las posibilidades de restringir la tipicidad. Además, el Convenio admite —no exige—como sanción la pena privativa de libertad. Un problema básico de ésto es que, si en el delito más leve, básico y de aplicación subsidiaria se usa la modalidad más grave de sanción; se caerá en problemas serios de proporcionalidad en el resto de las conductas. En realidad, se trata de un comportamiento sobre el que se discute si realmente es necesaria la intervención del derecho penal o si bastaría con la del contravencional o sancionador administrativo. Se estiman más lógicas las penas pecuniarias o de inhabilitación que la prisión.

b. Pasando a la recepción en el ámbito del Mercosur, puede señalarse que el "intrusismo informático" está expresamente tipificado en:

b.1 **Argentina**: por ley 26.388, lo ha incorporado al CP como artículo 153 *bis*.[23] La misma ley reformó el III del Título V —"Delitos contra la Libertad"—, que pasó a ser "Violación de Secretos y de la Privacidad", y dotó de una nueva redacción al artículo 157 *bis*, cuyo primer párrafo[24] pune el acceso ilegítimo a un banco de datos personales.

b.2 **Bolivia**: prevé en el artículo 363 *ter*[25] de su CP del año 1997, junto a la alteración y el uso indebido de datos informáticos, la punición del acceso

(23) "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" (art. 153 *bis* del CP).

(24) El texto vigente del art. 157 *bis,* en su parte pertinente, dice: "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…" (art. 157 *bis* del CP).

(25) Cuyo texto dice: "El que sin estar autorizado se apodere, acceda, utilice, modifique, suprima o inutilice, datos almacenados en una computadora o en cualquier soporte infor-

a aquellos datos informáticos alojados en una computadora o cualquier soporte informático.

b.3 **Colombia**: su CP —ley 599 de 2000— ha sido modificado por la ley 1273 de 2009. Ésta incorporó como capítulo VII *bis* uno específico para la delincuencia informática. El acceso abusivo a un sistema informático está contemplado en el artículo 269A.[26] Además debe tenerse presente que todas las conductas del capítulo tienen previstas una serie de circunstancia de agravación en el artículo final —269H—.[27]

b.4 **Ecuador**: a continuación del artículo 202 CPE, por ley 2002-67, se agregó un artículo sin número[28] cuyo primer segmento en su primer párrafo prevé el acceso u obtención de información protegida y, en el segundo, califica la conducta de acuerdo al tipo de información de que se trate.

mático, ocasionando perjuicio al titular de la información, será sancionado con prestación de trabajo hasta un año o multa hasta doscientos días" (art. 363 *ter.*).

(26) El nuevo artículo dice: "El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes".

(27) Su texto: "Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:

1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.
2. Por servidor público en ejercicio de sus funciones.
3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.
4. Revelando o dando a conocer el contenido de la información en perjuicio de otro.
5. Obteniendo provecho para sí o para un tercero.
6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional.
7. Utilizando como instrumento a un tercero de buena fe.
8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales".

(28) La parte pertinente dice: "art. ... (1). (Ag. por art. 58, ley 2002-67, RO 557-S, 17-IV-2002). El que empleando cualquier medio electrónico, informático o afín, violentare claves o sistemas de seguridad, para acceder u obtener información protegida, contenida en sistemas de información; para vulnerar el secreto, confidencialidad y reserva, o simplemente vulnerar la seguridad, será reprimido con prisión de seis meses a un año y multa de quinientos a mil dólares de los EU de Norteamérica.

Si la información obtenida se refiere a seguridad nacional, o a secretos comerciales o industriales, la pena será de uno a tres años de prisión y multa de mil a mil quinientos dólares de los Estados Unidos de Norteamérica".

b.5 **Paraguay**: conducta típica a partir de la reforma del CP por ley 4439 del año 2011, prevista en el nuevo artículo 174 b.[29]

b.6 **Perú**: había incorporado en su Parte Especial, por ley 27.309 —del 17 de julio de 2000—, en el Título V de los delitos contra el patrimonio; un X —"Delitos Informáticos"— con tres artículos. El primero de ellos (art. 207-A) punía, entre otras conductas, el ingreso indebido a una base de datos, sistema o red de computadoras, o cualquier parte de la misma con varias finalidades. Mientras que el último (art. 207-C) agravaba los anteriores en caso de que el acceso se hubiera logrado usando información privilegiada o se pusiera en peligro la seguridad nacional. El 22 de octubre de 2013 se publicó la nueva "Ley de Delitos Informáticos", bajo N° 30.096. Los mencionados artículos fueron derogados por su "disposición complementaria derogatoria única", a la vez que el "acceso ilícito" fue previsto en su artículo 2.[30]

b.7 **Venezuela**: prevé el "acceso indebido" en el artículo 6[31] de la "Ley Especial contra los Delitos Informáticos" (LECDI) del año 2001. A su vez, el artículo 9 establece como agravante que el sistema que utilice tecnologías de la información esté destinado a funciones públicas o contenga información personal o patrimonial de personas naturales o jurídicas, caso en que se incrementaría la pena entre una tercera parte y la mitad. A su vez, el artículo 21, referido a la violación de la privacidad de las comunicaciones, sanciona con pena de dos a seis años y multa de doscientas a seiscientas unidades tributaria al que, mediante el uso de las tecnologías de la información, acceda a cualquier mensaje de datos o señal de transmisión o comunicación ajena.

c. En cambio, no han modificado sus legislaciones:

c.1 **Brasil**: donde la conducta sería atípica. Aunque existe una salvedad en la regulación especial de su Ley Electoral N° 9100 del año 1995. El motivo fue la incorporación del sistema de voto electrónico en las elecciones de

(29) Con el siguiente texto: "Acceso indebido a datos. 1° El que sin autorización y violando sistemas de seguridad obtuviere para sí o para terceros, el acceso a datos no destinados a él y especialmente protegidos contra el acceso no autorizado, será castigado con pena privativa de libertad de hasta tres años o multa. 2° Como datos en sentido del inc. 1, se entenderán solo aquellos, que se almacenan o transmiten electrónicamente, magnéticamente o de otra manera no inmediatamente visible".

(30) Dice: "El que accede sin autorización a todo o parte de un sistema informático, siempre que se realice con vulneración de medidas de seguridad establecidas para impedirlo, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días multa. Será reprimido con la misma pena el que accede a un sistema informático excediendo lo autorizado" (art. 2).

(31) Su texto: Toda persona que "sin la debida autorización o excediendo la que hubiere obtenido, acceda, intercepte, interfiera o use un sistema que utilice tecnologías de infor-

1996; por lo que se introdujo (art. 67 inc. VII) un tipo penal para punir con reclusión de uno a dos años y multa la obtención indebida de acceso, o su intento, a un sistema de tratamiento automatizado de datos utilizado por el servicio electoral con el fin de alterar el cómputo o cálculo de votos.

c.2 **Chile**: tampoco lo prevé en forma directa.

c.3 **Uruguay**: no hay un tipo específico, pero se ha verificado una condena por esta conducta —subsumida bajo la figura del artículo 300 del CP—,[32] que pena el "conocimiento fraudulento de secretos", aparentemente más apto para los casos de intercepción ilícita.

2.2 | Interceptación ilícita (art. 3)

> "Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, 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. Las Partes podrán exigir que la infracción sea cometida con alguna intención delictiva o también podrán requerir que la infracción se perpetre en un sistema informático conectado a otro sistema informático".[33]

a. Al igual que en el caso anterior, el Convenio contempla que los signatarios incorporen la conducta descripta sujetando su tipicidad a la exigencia

mación, será pena con prisión de uno a cinco años y multa de diez a cincuenta unidades tributarias".

(32) Dice: "El que, por medios fraudulentos, se enterare del contenido de documentos públicos o privados que por su propia naturaleza debieran permanecer secretos, y que no constituyeran correspondencia, será castigado, siempre que del hecho resultaren perjuicios, con multa de 20 U.R. (veinte unidades reajustables) a 400 U.R. (cuatrocientas unidades reajustables)"..

(33) Si bien la DM del año 2005 mencionada respecto del anterior artículo no previó equivalente al ahora transcripto, su sustituta Directiva 2013/40/UE del Parlamento Europeo y del Consejo de 12 de agosto de 2013 relativa a los ataques contra los sistemas de información, ha reafirmado la propuesta típica en su artículo 6°: "Los Estados miembros adoptarán las medidas necesarias para garantizar que la interceptación, por medios técnicos, de transmisiones no públicas de datos informáticos hacia, desde o dentro de un sistema de información, incluidas las emisiones electromagnéticas de un sistema de información que contenga dichos datos informáticos, intencionalmente y sin autorización, sea sancionable como infracción penal, al menos en los casos que no sean de menor gravedad".

de alguna intención delictiva, o que se perpetre con relación a un sistema informático interconectado. Pero, sin embargo, cuando se han dado casos de tipificación posterior, no se observa la adopción de tales limitaciones.

b. En los países del Mercosur se observa lo siguiente:

b.1 **Argentina**: la protección de las comunicaciones por vía electrónica se procura a través del concurso de diferentes normas. Para ello se distinguen dos perspectivas: las que afectan el secreto y la privacidad, y las que conciernen a la seguridad del medio de comunicación mismo —pertinentes a los fines del art. 5 de Budapest—. En consecuencia, se han sustituido o incorporado tipos en los s respectivos de la parte especial.

En lo que hace a la "Violación de secretos y de la privacidad", con la ley 26.388 —año 2008 — se cerró la discusión concerniente a la protección o desprotección penal del correo electrónico, sustituyendo al 153 del CP;[34] incluyendo el tema de la publicación abusiva de correspondencia para que alcance a la "comunicación electrónica" con la sustitución del artículo 155.[35]

b.2 **Brasil**: los e-mails tienen parcial protección en el artículo 151 del CP, con alguna discusión en cuanto a la exigencia de que la correspondencia esté "cerrada"; mientras que serían atípicas las conductas de suprimir, agregar o modificar el contenido del mensaje. Túlio L. Vianna opina en contra de la subsunción en el artículo 151 citado, aunque propició otra por la que la correspondencia electrónica tiene protección penal, partiendo del propio artículo 5°, XII de la Constitución Federal, que incluyó la inviolabilidad y

(34) Tiene ahora el siguiente texto: "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".

(35) Su redacción actual: "Será reprimido con multa de pesos un mil quinientos ($ 1500) 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".

secreto de la comunicación de datos.[36] Sostiene que el delito de violación de mails está tipificado en el marco de la genérica redacción del artículo 56 del Código Brasilero de Telecomunicaciones[37] —ley 4117 de 27 de agosto de 1962—, en función del artículo 58 del mismo texto, que deriva a la pena del mencionado artículo 151 del CP —detención de uno a seis meses o multa—; además de fijar algunas particulares para los concesionarios o permisionarios —elevando hasta uno a dos años de detención—. Se trata, simplemente, de un agente que efectivamente recoge o toma el mensaje del servidor sin autorización legal o reglamentaria.

En el artículo 10 de la ley 9296 del 24 de julio de 1996 —que reglamenta el citado artículo 5° CF—, se tipificó la conducta de quien realiza intercepción de comunicación telefónica, informática o telemática; o viola el secreto de justicia sin autorización judicial o con objetivos no autorizados legalmente.[38] Para Vianna, esta norma —que prevé la reclusión de dos a cuatro años y multa— vino, aparentemente, a aumentar la pena del delito de violación de e-mails. Al ser la "interceptación" una acción típica, concluye que sólo serán aprehendidos por esta figura los casos en que el autor impida que el mensaje llegue intacto al destinatario. Por eso, los supuestos casos en los que simplemente se acceda al servidor y se lea los mails, sin modificar o borrarlos, no serían intercepciones ya que no interrumpirían el curso del mensaje. De allí que sostenga que la mera lectura o copia de mails deben ser encuadrados en los citados artículos 56 y 58 del Código Brasilero de Telecomunicaciones (parág. 2.4).

b.3 **Chile**: contempla el que denomina "Espionaje informático" en el artículo 2° de la ley 12.223 del año 2003.

b.4 **Colombia**: en su CP —ley 599, del año 2000—, por ley 1273 de 2009, se incorporó la figura de interceptación de datos informáticos en el artículo 269C.[39]

(36) Vianna, Túlio Lima, "Dos crimes por computador", [en línea] www.mundojuridico.adv.br, en 16/4/03. La parte pertinente del artículo citado de la C.F. dice: *"é inviolavel o sigilo da correspondencia e das comunicações telegráficas, de dados e das comunicações telefônicas…"*.

(37) Dice: "Pratica crime de violação de telecomunicações quem, transgredindo lei ou regulamento, exiba autógrafo ou qualquer documento ou arquivo, divulgue ou comunique, informe ou capte, transmita a outrem ou utilize o conteúdo, resumo, significado, interpretação, indicação ou efeito de qualquer comunicação dirigida a terceiro"..

(38) Ver Lopes da Silva, "Direito Penal e Sistema Informático", en *Editora Revista dos Tribunais, Série Ciência do Direito Penal Contemporânea*, vol. 4, San Pablo, Brasil, 2003, p. 70.

(39) Su texto: "El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses".

b.5 **Ecuador**: la interceptación de las comunicaciones está prevista en el artículo 197[40] de su CP. Además, a continuación del artículo 202 CPE se agregó por ley 2002-67 un artículo sin número[41] que tiene dos segmentos. En los párrafos tres y cuatro del primero de ellos, se pune la violación de secretos comerciales o industriales y se agrava la conducta de divulgación o utilización fraudulenta si es perpetrada por persona encargada de la custodia o utilización legítima de datos. En el segundo segmento, se tipifica directamente la obtención y uso no autorizado de información sobre datos personales.

En materia de delitos comunes de la función policial o militar, por ley sin número del 19 de mayo de 2010, se introdujo un artículo sin número[42] a

(40) Dice: "art. 197 (Sustituido por el art. 2° de la ley s/n, R.O. 555-S, 24-III-2009). Serán sancionados con penas de 2 meses a un año de prisión, quienes interceptaren sin orden judicial, conversaciones telefónicas o realizadas por medios afines y quienes se sustrajeran o abrieran sobres de correspondencia que pertenecieren a otro sin autorización expresa. Se exime la responsabilidad de quien lo hizo cuando la interceptación telefónica o la apertura de sobres se produce por error, en forma accidental o fortuita".

(41) Su parte pertinente dice: "art. ... (1). ...La divulgación o la utilización fraudulenta de la información protegida, así como de los secretos comerciales o industriales, será sancionada con pena de reclusión menor ordinaria de tres a seis años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica. Si la divulgación o la utilización fraudulenta se realiza por parte de la persona o personas encargadas de la custodia o utilización legítima de la información, éstas serán sancionadas con pena de reclusión menor de seis a nueve años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica.

art. … (2). (Ag. por art. 58, ley 2002-67, R.O. 557-S, 17-IV-2002). Obtención y utilización no autorizada de información. La persona o personas que obtuvieren información sobre datos personales para después cederla, publicarla, utilizarla o transferirla a cualquier título, sin la autorización de su titular o titulares, serán sancionadas con pena de prisión de dos meses a dos años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica".

(42) Sus textos: "art. … (602.11). Violación de correspondencia. (Agregado por el art. 4° de la ley s/n, R.O. 196-S, 19-V-2010). Será sancionado con prisión de tres meses a un año, la servidora o servidor militar o policial que, sin la debida autorización legal, intercepte, examine, retenga, grabe o difunda correspondencia o comunicaciones privadas o reservadas de cualquier tipo y por cualquier medio".

"art. … (602.12). Delitos contra la información pública no clasificada legalmente. (Agregado por el art. 4 de la ley s/n, R.O. 196-S, 19-V-2010). Será sancionado con prisión de tres meses a un año, la servidora o servidor militar o policial que, utilizando cualquier medio electrónico, informático o afín, obtenga información a la que tenga acceso en su condición de servidora o servidor policial o militar, para después cederla, publicarla, divulgarla, utilizarla o transferirla a cualquier título sin la debida autorización. La misma pena será aplicable a quien destruyere o inutilizare este tipo de información.

Si la divulgación o la utilización fraudulenta son realizadas por cualquier persona o personas encargadas de la custodia o utilización legítima de la información, éstas serán sancionadas con el máximo de la pena".

"art. … (602.13). Delitos contra la información pública clasificada legalmente. (Agregado por el art. 4 de la ley s/n, R.O. 196-S, 19-V-2010). Será sancionado con reclusión menor ordinaria

continuación del artículo 602 del CP, cuyos segmentos undécimo a décimo tercero consagran tipos especiales de violación de correspondencia y contra la información pública clasificada o no clasificada legalmente.

b.6 **Paraguay**: por vía de la reciente ley 4439 —año 2011—, se incorporó la interceptación de datos como nuevo artículo 146 c[43] a su CP. Con carácter previo, puede mencionarse la existencia de regulación vinculada al secreto de empresa, que tiene protección penal expresa conforme el Código Penal de 1997 en el capítulo VII —"Hechos punibles contra el ámbito de la vida y la intimidad de la persona"—, en el artículo 147 —"Revelación de un secreto de carácter privado"—.[44]

b.7 **Perú**: el artículo 207-A del CP de 1991 —conforme ley 27.309 del 17 de julio de 2000— punía, entre otras conductas, el uso o ingreso indebido a una base de datos, sistema, red de computadoras o cualquier parte de la misma con finalidad de interferir, interceptar, acceder o copiar información en tránsito o contenida en una base de datos. Regían también los agravantes del artículo 207-C. Fueron derogados mediante la "disposición complementaria derogatoria única" de la ley 30.096 de 2013; por la que ha pasado a ser el tipo aplicable el de su artículo 7° —"Interceptación de datos informáticos"—,[45] que integra su capítulo IV —"Delitos informáticos

de tres a seis años, la servidora o servidor militar o policial que, utilizando cualquier medio electrónico, informático o afín, obtenga información clasificada de conformidad con la ley. La misma pena será aplicable a quien destruyere o inutilizare este tipo de información.

Si la divulgación o la utilización fraudulenta son realizadas por cualquier persona o personas encargadas de la custodia o utilización legítima de la información, éstas serán sancionadas con el máximo de la pena".

(43) El texto introducido al CP es el siguiente: "Art. 146 c. Interceptación de datos. El que, sin autorización y utilizando medios técnicos: 1° obtuviere para sí o para un tercero, datos en sentido del art. 146 b, inc. 2, no destinados para él; 2° diera a otro una transferencia no pública de datos; o 3° transfiriera la radiación electromagnética de un equipo de procesamiento de datos, será castigado con pena privativa de libertad de hasta dos años o multa, salvo que el hecho sea sancionado por otra disposición con una pena mayor".

(44) Cuya parte pertinente reza: "1° El que revelara un secreto ajeno: 1. llegado a su conocimiento en su actuación como, a) médico, dentista o farmacéutico; b) abogado, notario o escribano público, defensor en causas penales, auditor o asesor de Hacienda; c) ayudante profesional de los mencionados anteriormente o persona formándose con ellos en la profesión; o 2. respecto del cual le incumbe por ley o en base a una ley una obligación de guardar silencio, será castigado con pena privativa de libertad de hasta un año o con multa. ...3° Cuando el secreto sea de carácter industrial o empresarial, la pena privativa de libertad podrá ser aumentada hasta tres años. Será castigada también la tentativa".

(45) Dice: "El que a través de las tecnologías de la información o de la comunicación, intercepta datos informáticos en transmisiones no públicas, dirigidas a un sistema informático, originadas en un sistema informático o efectuadas dentro del mismo, incluidas las emisiones

contra la intimidad y el secreto de las comunicaciones"—. Se complementa con el artículo 6°,[46] que pune el "Tráfico ilegal de datos".

b.8 **Uruguay**: por ley 18.383 —del 17de octubre de 2008—, se modificó el artículo 217[47] del CP, a partir del que se pena al atentado contra la regularidad de las telecomunicaciones. A su vez, por ley 18.515 —del 26 de junio de 2009—, se volvieron a modificar los artículos del CP relativos a la protección de los medios de comunicación. Además, puede acotarse que por ley 18.494 —del 5 de junio de 2009— se modificó el régimen sobre prevención y control de lavados de activos y del financiamiento del terrorismo, regulándose lo relativo a las vigilancias electrónicas "legales".

b.9 **Venezuela**: prevé el espionaje informático en el artículo 11[48] de su LECDI del año 2001. Tiene, además, una figura de "hurto" (art. 13)[49] y, en el citado artículo 21, referido a la violación de la privacidad de las comunicacio-

electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años.

La pena privativa de libertad será no menor de cinco ni mayor de ocho años cuando el delito recaiga sobre información clasificada como secreta, reservada o confidencial de conformidad con las normas de la materia.

La pena privativa de libertad será no menor de ocho ni mayor de diez años cuando el delito comprometa la defensa, la seguridad o la soberanía nacionales".

(46) Dice: "El que crea, ingresa o utiliza indebidamente una base de datos sobre una persona natural o jurídica, identificada o identificable, para comercializar, traficar, vender, promover, favorecer o facilitar información relativa a cualquier ámbito de la esfera personal, familiar, patrimonial, laboral, financiera y otro de naturaleza análoga, creando o no perjuicio, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años".

(47) Su texto actual: "El que, de cualquier manera, atentare contra la regularidad de las comunicaciones telefónicas, telegráficas o inalámbricas, poniendo en peligro la seguridad de los transportes públicos, será castigado con tres meses de prisión a tres años de penitenciaría".

(48) Dice que toda persona: "... que indebidamente obtenga, revele o difunda la data o información contenidas en un sistema que utilice tecnologías de la información o en cualesquiera de sus componentes, será penada con prisión de tres a seis años y multa de trescientas a seiscientas unidades tributarias. La pena se aumentará de un tercio a la mitad, si el delito previsto en el presente artículo se cometiere con el fin de obtener algún tipo de beneficio para sí o para otro.

El aumento será de la mitad a dos tercios, si se pusiere en peligro la seguridad del Estado, la confiabilidad de la operación de las instituciones afectadas o resultare algún daño para las personas naturales o jurídicas, como consecuencia de la revelación de las informaciones de carácter reservado".

(49) Su texto: "El que a través del uso de tecnologías de la información, acceda, intercepte, interfiera, manipule o use de cualquier forma un sistema o medio de comunicación para apoderarse de bienes o valores tangibles o intangibles de carácter patrimonial sustrayéndolos a su tenedor, con el fin de procurarse un provecho económico para sí o para otro, será sancionado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias".

nes; sanciona al que mediante el uso de las tecnologías de la información capture o interfiera cualquier mensaje de datos o señal de transmisión o comunicación ajena con pena de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

c. En cambio no se advierten normas específicas en **Bolivia**, ya que su CP de 1997 sólo tipifica las tradicionales violaciones de secretos (arts. 300/302).

2.3 | Atentados contra la integridad de los datos (art. 4)

"1. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, la conducta de dañar, borrar, deteriorar, alterar o suprimir dolosamente y sin autorización los datos informáticos.

2. Las Partes podrán reservarse el derecho a exigir que el comportamiento descrito en el párrafo primero ocasione daños que puedan calificarse de graves". (50)

a. En este caso, resaltan de la Mata Barranco y Hernández Díaz, se otorga protección directa únicamente a los elementos lógicos de los sistemas informáticos sin especificar cómo debe ser la modalidad de ataque, contemplando conductas que no implican necesariamente la destrucción de un objeto sino, simplemente, la variación del contenido de un dato. (51)

Vale enfatizar que la propuesta de tipificación de las conductas que importan atentados contra la integridad de datos admite ese límite exigiendo que, para la intervención penal, se trate de la producción de daños graves.

(50) Esta propuesta típica fue reafirmada mediante la Decisión Marco 2005/222/JAI del Consejo, de 24 de febrero de 2005, relativa a los ataques contra los sistemas de información, con esta redacción: "Artículo 4. Intromisión ilegal en los datos. Cada Estado miembro adoptará las medidas necesarias para que el acto intencionado, cometido sin autorización, de borrar, dañar, deteriorar, alterar, suprimir o hacer inaccesibles datos informáticos contenidos en un sistema de información sea sancionable como infracción penal, al menos en los casos que no sean de menor gravedad". A su vez, ha sido sustituido por el art. 5° de la Directiva 2013/40/UE del Parlamento Europeo y del Consejo de 12 de agosto de 2013 relativa a los ataques contra los sistemas de información, "Interferencia ilegal en los datos", manteniendo similar redacción.

(51) De la Mata Barranco, Norberto J.; Hernández Díaz, Leyre, "El delito de daños informáticos: una tipificación defectuosa", en *Estudios Penales y Criminológicos*, Servicio de Publicaciones de la Universidad de Santiago de Compostela, vol. XXIX, 2009, p. 322.

Ésto, para aquellos países imbuidos de la tradicional dogmática continental europea, es una fórmula que les permite tipificar en forma congruente con el principio de lesividad y dejar afuera del derecho penal las afectaciones bagatelares o menores. Como destaca Morales García tomando como ejemplo del artículo 260 del CPE, en muchos casos se trasluce en la adopción de una cuantía económica mínima como perjuicio para expresar penalmente el desvalor de la conducta. El problema puede presentarse al momento de precisar qué se debe tomar como referencia para la valoración del daño: ¿el valor en sí mismo del dato informático? Y, si es así, ¿cómo lo mensuro?, ¿se tomará el valor de cambio del dato informático? Si fuera de ese modo, ¿qué pasa con la destrucción de un dato respecto del que existe copia de seguridad, en cuyo caso el valor de cambio permanecería inalterado?, ¿sería un caso de tentativa posible y punible, o imposible e impune?[52] Puede anticiparse que en ninguna de las normas sudamericanas que seguidamente se indicarán se ha optado por fijar una cuantía para deslindar entre un daño delictivo y otro contravencional.

b. Al bucear en las legislaciones regionales, puede advertirse la presencia de tipos específicos en:

b.1 **Argentina**: donde la reforma por ley 26.388 —año 2008— incorporó el daño en datos, documentos, programas o sistemas informáticos mediante un segundo párrafo agregado al artículo 183[53] y la sustitución del artículo 184[54] del CP.

Previamente, había sido normada la "alteración dolosa de registros fiscales" en el artículo 12[55] de la vigente Ley Penal Tributaria y Previsional

(52) Morales García, *op. cit.*, p. 30.

(53) Dice: "… 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" (2° párr.).

(54) Con este texto: "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".

(55) El tipo del régimen especial dice: "Será reprimido con prisión de dos a seis años, el que de cualquier modo sustrajere, suprimiere, ocultare, adulterare, modificare o inutilizare los registros o soportes documentales o informáticos del fisco nacional, relativos a las obligaciones

Nro. 24.769 —año 1997—. Luego, se amplió la tipificación por la incorporación de la "alteración dolosa de sistemas informáticos o equipos electrónicos" como artículo 12 *bis*,[56] por ley 26.735 de fines de 2011.

La inserción o la inducción a la inserción ilegítima de datos en un archivo de datos personales comenzó a punirse con la modificación del CP por la LPDP del año 2000. Pero el artículo 157 *bis* fue nuevamente reformado por la citada ley 26.388; quedando como su inc. 3°,[57] que agrava la conducta cuando es desplegada por un funcionario público.

La protección de datos personales se complementa, más allá de lo que requiere Budapest, con una actualizada sección dedicada a la violación de secretos. En el citado art. 157 *bis* inc. 2° se pune también al que "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". A su vez, la simple revelación de secretos del art. 157[58] también fue actualizada por ley 27.388 incluyendo la palabra "datos".

b.2 **Bolivia**: la modificación, supresión o inutilización de datos está contemplada en el ya transcripto artículo 363 *ter*[59] del CP de 1997.

b.3 **Brasil**: presenta una situación similar a la Argentina antes de la reforma de 2008 en relación al delito de daño. La discusión giraba alrededor del artículo 163 del CP de 1940,[60] por lo que podía considerarse sin tipo

tributarias o de recursos de la seguridad social, con el propósito de disimular la real situación fiscal de un obligado".

(56) Con esta redacción: "Será reprimido con prisión de uno (1) a cuatro (4) años, el que modificare o adulterare los sistemas informáticos o equipos electrónicos, suministrados u homologados por el fisco nacional, provincial o de la Ciudad Autónoma de Buenos Aires, siempre y cuando dicha conducta fuere susceptible de provocar perjuicio y no resulte un delito más severamente penado".

(57) El segmento pertinente del art. 157 *bis* dice: "Será reprimido con la pena de prisión de un (1) mes a dos (2) años el que: (…) 3. Ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales. Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de un (1) a cuatro (4) años".

(58) Ahora dice: "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".

(59) Su texto: "Alteración, acceso y uso indebido de datos informáticos. El que sin estar autorizado se apodere, acceda, utilice, modifique, suprima o inutilice, datos almacenados en una computadora o en cualquier soporte informático, ocasionando un perjuicio al titular de la información, será sancionado con prestación de trabajo hasta un año o multa de hasta doscientos días".

(60) Dice: "art. 163. *Destruir, inutilizar ou deteriorar coisa alheia: Pena – detenção, de 1 (um) a 6 (seis) meses, ou multa*".

expreso. Pero debe ahora tenerse presente la posible concurrencia para subsumir algunos casos del art. 154-A del CPB conforme a la ley 12.737; así, la destrucción de daños o informaciones en dispositivo informático.

También a semejanza del caso argentino, por ley 9983 —año 2000—, se introdujo un tipo de violación de secretos calificado por vía de la modificación de los artículos 153 y 325 del CPB. En efecto, el artículo 153, parág. 1°, letra "A" —"Violación de secreto"—, prevé pena de detención de 1 a 4 años y multa para el que divulgue, sin justa causa, informaciones secretas o reservadas, así definidas por ley, contenidas en sistemas informáticos o bancos de datos de la Administración Pública. Mientras que el art. 325, parágs. 1° y 2° —"Violación de secreto funcional"—, prevé pena de detención de 6 meses a 2 años o multa para el que permitiere o facilitare mediante atribución, provisión y préstamo de clave o cualquier otra forma, el acceso de persona no autorizada a sistemas informáticos o banco de datos de la Administración Pública; o utilizare, indebidamente, el acceso restringido. Califica por daño a la Administración Pública o a otro, con pena de reclusión de 2 a 6 años y multa.

Dentro del marco de los delitos contra la Administración Pública, la ley citada agregó al CPB los artículos 313-A[61] y 313-B,[62] con los que vino a tutelar la seguridad de los sistemas de información de aquélla exclusivamente. Es decir, sus previsiones no son aplicables a los sistemas de informaciones de entidades particulares o privadas.

Por ley 12.737 —año 2012— se ha incorporado la protección de los secretos comerciales o industriales, la información secreta definida por ley y las comunicaciones electrónicas privadas mediante la reforma introducida al artículo 154-A del CP —ley 2848 del 7 de diciembre de 2004—. Además, por ley 12.737, un nuevo parágrafo (parág. 3º) prevé pena de reclusión de seis meses a dos años y multa, siempre que no constituya un delito más grave. Se agrava de uno a dos tercios si media divulgación, comercialización o transmisión a terceros a cualquier título de los datos obtenidos (parág. 4º).

b.4 **Chile**: la ley 19.223 —año1993— contempla el "Sabotaje informático" en su artículo 1°.[63] El primer párrafo describe la conducta básica, mientras que el segundo agrava cuando se afectan datos contenidos en un sistema.

(61) Su redacción: *"Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano: Pena- reclusão de 2(dois) a 12 (doze) anos e multa"*.

(62) Dice: *"Modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente"*. Se prevé pena de 3 meses a dos años de detención y multa. Además, califica agravando la pena de un tercio a la mitad si de ello resulta daño para la administración pública o un administrado (parágrafo único final).

(63) Su redacción: "El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcio-

b.5 **Colombia**: su CP, reformado en 2009 por ley 1273, en materia de integridad de datos, prevé el "daño informático" en el artículo 269D.[64] A su vez, en el artículo 269F[65] se pune la "violación de datos personales" y en el artículo 269G[66] la "suplantación de sitios web para capturar datos personales".

b.6 **Ecuador**: por ley 2002-67 se sustituyó el texto del artículo 262[67] de su Código Penal, incluyendo la destrucción o supresión dolosa de programas, datos, bases de datos, etc.; en caso de su comisión por empleado público o persona encargada de su guarda. Además, por la misma ley se agregó, a continuación del artículo 415 del CPE, un artículo sin número,[68] en cuyo primer párrafo tipifica los daños informáticos y, agra-

namiento, sufrirá la pena de presidio menor en su grado medio a máximo. Si como consecuencia de estas conductas se afectaren datos contenidos en un sistema, se aplicará la pena señalada en el inciso anterior, en su grado máximo".

(64) Su texto: "El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes".

(65) Dice: "El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes".

(66) Su texto: "El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.

En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave.

La pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito".

(67) Su texto actual: "Serán reprimidos con tres a seis años de reclusión menor, todo empleado público y toda persona encargada de un servicio público, que hubiere maliciosa y fraudulentamente, destruido o suprimido documentos, títulos, programas, datos, bases de datos, información o cualquier mensaje de datos con-tenido en un sistema de información o red electrónica, de que fueren depositarios, en su calidad de tales, o que les hubieren sido encomendados en razón de su cargo".

(68) Dice: "art. ... (1). (Ag. por art. 61, L. 2002-67, R.O. 557-S, 17-IV-2002). Daños informáticos. El que dolosamente, de cualquier modo o utilizando cualquier método, destruya, altere, inutilice, suprima o dañe, de forma temporal o definitiva, los programas, datos, bases de

va cuando recae sobre sistema vinculado a servicios públicos o defensa en el segundo.

b.7 **Paraguay**: pune mediante el artículo 174[69] de su CP la "alteración de datos". Encuentra complemento en el siguiente, rebautizado por ley 4439 del año 2011 como "Sabotaje a sistemas informáticos"[70] que, conforme el texto actual, ya no exige que los datos sean de importancia vital y se incorporan a los particulares como objetos de posible ataque.

A su vez, ya en versión original del código, se dedicaron dos artículos a los hechos punibles contra la prueba documental en los que se alude a la alteración de datos y conectan expresamente con el inc. 3° del artículo 174, antes citado. Se trata de los artículos 248[71] y 249.[72]

b.8 **Perú**: la alteración, daño y destrucción de base de datos, se incorporó al CP de 1991 por ley 27.309 el 17 de julio de 2000 como nuevo artículo 207-B. Recibió los agravantes del artículo 207-C. Luego, fueron derogados por la

datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, será reprimido con prisión de seis meses a tres años y multa de 60 a 150 dólares de los EUN.

La pena de prisión será de tres a cinco años y multa de 200 a 600 dólares…, cuando se trate de programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, destinada a prestar un servicio público o vinculada con la defensa nacional".

(69) Su texto: "Artículo 174. Alteración de datos. 1) El que lesionando el derecho de disposición de otro sobre datos los borrara, suprimiera, inutilizara o cambiara, será castigado con pena privativa de libertad de hasta dos años o con multa. 2) En estos casos, será castigada también la tentativa. 3) Como datos, en el sentido del inc. 1, se entenderán sólo aquellos que sean almacenados o se transmitan electrónica o magnéticamente, o en otra forma no inmediatamente visible".

(70) La nueva redacción es: "Artículo 175. 1° El que obstaculizara un procesamiento de datos de un particular, de una empresa, asociación o de una entidad de la administración pública, mediante: 1) un hecho punible según el art. 174, inc. 1; o 2) la destrucción, inutilización, sustracción o alteración de una instalación de procesamiento de datos, de una unidad de almacenamiento o de otra de sus partes componentes indispensable. será castigado con pena privativa de libertad de hasta cinco años o con multa. 2° En estos casos será castigada también la tentativa".

(71) Su texto: "Artículo 248. Alteración de datos relevantes para la prueba. 1) El que con la intención de inducir al error en las relaciones jurídicas, almacenara o adulterara datos en los términos del art. 174, inc. 3, relevantes para la prueba de tal manera que, en caso de percibirlos se presenten como un documento no auténtico, será castigado con pena privativa de libertad de hasta cinco años o con multa. 2) En estos casos será castigada también la tentativa. 3) En lo pertinente se aplicará también lo dispuesto en el art. 246, inc. 4".

(72) Dice: "Artículo 249. Equiparación para el procesamiento de datos. La manipulación que perturbe un procesamiento de datos conforme al art. 174, inc. 3, será equiparada a la inducción al error en las relaciones jurídicas".

"disposición complementaria derogatoria única" de la ley 30.096 de 2013, cuyo artículo 3° —"Atentado contra la integridad de datos informáticos"— es el tipo actualmente regente.[73]

Además, en general, la violación de la intimidad está tipificada en el artículo 154 del CP y se prevé autónomamente la punición del uso indebido de archivos computarizados (art. 157).[74] El tipo referido a la interferencia telefónica (art. 162)[75] ha sido expresamente modificado conforme la disposición complementaria modificatoria "cuarta" de la ley 30.096 mencionada.

b.9 **Venezuela**: en el capítulo I de su LECDI de 2001 —"De los delitos contra los sistemas que utilizan tecnologías de la información"—, se prevé el sabotaje o daño a sistemas, tanto en su forma dolosa (art. 7°);[76] como culposa (art. 8°);[77] considerándose agravada la conducta de acceso indebido

(73) Dice: "El que, a través de las tecnologías de la información o de la comunicación, introduce, borra, deteriora, altera, suprime o hace inaccesibles datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días multa".

(74) Su texto: "El que, indebidamente, organiza, proporciona o emplea cualquier archivo que tenga datos referentes a las convicciones políticas o religiosas y otros aspectos de la vida íntima de una o más personas, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años.
Si el agente es funcionario o servidor público y comete el delito en ejercicio del cargo, la pena será no menor de tres ni mayor de seis años e inhabilitación conforme al art. 36, incs. 1, 2 y 4".

(75) El nuevo texto dice: "El que, indebidamente, interfiere o escucha una conversación telefónica o similar será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años.

Si el agente es funcionario público, la pena privativa de libertad será no menor de cuatro ni mayor de ocho años e inhabilitación conforme al art. 36, incs. 1, 2 y 4.

La pena privativa de libertad será no menor de cinco ni mayor de ocho años cuando el delito recaiga sobre infracción clasificada como secreta, reservada o confidencial de conformidad con las normas de la materia. La pena privativa de libertad será no menor de ocho años ni mayor de diez años cuando el delito comprometa la defensa, la seguridad o la soberanía nacionales".

(76) Dice: "Artículo 7. Sabotaje o daño a sistemas. El que destruya, dañe, modifique o realice cualquier acto que altere el funcionamiento o inutilice un sistema que utilice tecnologías de información o cualquiera de los componentes que lo conforman, será penado con prisión de cuatro a ocho años y multa de cuatrocientas a ochocientas unidades tributarias.

Incurrirá en la misma pena quien destruya, dañe, modifique o inutilice la data o la información contenida en cualquier sistema que utilice tecnologías de información o en cualquiera de sus componentes. La pena será de cinco a diez años de prisión y multa de quinientas a mil unidades tributarias, si los efectos indicados en el presente artículo se realizaren mediante la creación, introducción o transmisión, por cualquier medio, de un virus o programa análogo".

(77) Se transcribe. "Artículo 8. Sabotaje o daño culposos. Si el delito previsto en el artículo anterior se cometiere por imprudencia, negligencia, impericia o inobservancia de las normas

o sabotaje cuando se trate de sistemas protegidos destinados a funciones públicas o con información personal o patrimonial de personas naturales o jurídicas en el ya referido artículo 9°. Vale enfatizar que, mientras el Convenio reclama la punición de la conducta a título doloso; la legislación venezolana va mucho más allá al punir también daños imprudentes.

En el capítulo III —"De los delitos contra la privacidad de las personas y de las comunicaciones"— de la LECDI de 2001, hay otras normas protectoras, tanto de la integridad como del secreto de los datos personales: los delitos de violación de la privacidad de la data o información de carácter personal (art. 20);[78] violación de la privacidad de las comunicaciones (art. 21)[79] y la revelación indebida de data o información de carácter personal (art. 22).[80]

La siguiente norma de la Constitución de 1999 opera de pauta interpretativa al establecer, con respecto a la posibilidad de grabar comunicaciones y emplearlas como medios probatorios en juicio, lo siguiente:

"Se garantiza el secreto e inviolabilidad de las comunicaciones privadas en todas sus formas. No podrán ser interferidas sino por orden de un tribunal competente, con el cumplimiento de las disposiciones legales y preservándose el secreto de lo privado que no guarde relación con el correspondiente proceso"(art. 48).

c. En cambio, no se ha producido aún una reforma que se ocupe de esta propuesta típica en **Uruguay**. Por lo que allí se mantendría la discutida

establecidas, se aplicará la pena correspondiente según el caso, con una reducción entre la mitad y dos tercios".

(78) Tiene la siguiente redacción: "Artículo 20. Violación de la privacidad de la data o información de carácter personal. Toda persona que intencionalmente se apodere, utilice, modifique o elimine por cualquier medio, sin el consentimiento de su dueño, la data o información personales de otro o sobre las cuales tenga interés legítimo, que estén incorporadas en un computador o sistema que utilice tecnologías de información, será penada con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

La pena se incrementará de un tercio a la mitad si como consecuencia de los hechos anteriores resultare un perjuicio para el titular de la data o información o para un tercero".

(79) En lo pertinente, ya que lo contempla entre otras conductas, sanciona al que mediante el uso de las tecnologías de la información reproduzca, modifique o elimine cualquier mensaje de datos o señal de transmisión o comunicación ajena, con pena de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

(80) Con la siguiente redacción: "Artículo 22. Revelación indebida de data o información de carácter personal. Quien revele, difunda o ceda, en todo o en parte, los hechos descubiertos, las imágenes, el audio o, en general, la data o información obtenidos por alguno de los medios indicados en los arts. 20 y 21, será sancionado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

Si la revelación, difusión o cesión se hubieren realizado con un fin de lucro, o si resultare algún perjuicio para otro, la pena se aumentará de un tercio a la mitad".

situación de la capacidad de rendimiento para subsumir estas conductas en las tradicionales figuras de "daño". Puede acotarse que allí se ha sancionado el 11 de agosto de 2008 la Ley 18331 de Protección de Datos Personales, cuyo artículo 1° comienza reconociéndoles estatus de derecho humano fundamental —"el derecho a la protección de datos personales es inherente a la persona humana…"—, aplicable por extensión a las personas jurídicas (ver art. 2°). Entre otros principios que rigen la tutela de datos personales está el de reserva (art. 11), enfatizado por la remisión al artículo 302[81] de CP en cuanto a la estrecha guarda del secreto profesional.

2.4 | Atentados contra la integridad del sistema (art. 5)

> "Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, la obstaculización grave, cometida de forma dolosa y sin autorización, del funcionamiento de un sistema informático, mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos".[82]

a. Al considerar no ya las afectaciones a la integridad de datos, sino del sistema; pueden verificarse tipos específicos en:

a.1 **Argentina**: en el marco de la reforma generalizada del CP por vía de la ley 26.388, en materia de "Delitos contra la seguridad de los medios de

(81) Dice: "El que, sin justa causa, revelare secretos que hubieran llegado a su conocimiento, en virtud de su profesión, empleo o comisión, será castigado, cuando el hecho causare perjuicio, con multa de 100 U.R. (cien unidades reajustables) a 600 U.R. (seiscientas unidades reajustables)".

(82) Esta propuesta típica, ampliando al incluir la directa interrupción, fue reafirmada mediante la Decisión Marco 2005/222/JAI del Consejo, de 24 de febrero de 2005, relativa a los ataques contra los sistemas de información, con esta redacción: "Artículo 3. Intromisión ilegal en los sistemas de información. Cada Estado miembro adoptará las medidas necesarias para que el acto intencionado, cometido sin autorización, de obstaculizar o interrumpir de manera significativa el funcionamiento de un sistema de información, introduciendo, transmitiendo, dañando, borrando, deteriorando, alterando, suprimiendo o haciendo inaccesibles datos informáticos, sea sancionable como infracción penal, al menos en los casos que no sean de menor gravedad". A su vez, ha sido sustituido por el art. 4 de la Directiva 2013/40/UE del Parlamento Europeo y del Consejo de 12 de agosto de 2013 relativa a los ataques contra los sistemas de información, "Interferencia ilegal en los sistemas de información", manteniendo una redacción similar.

transporte y de comunicación", se ha sustituido el artículo dedicado a la "Interrupción o resistencia al restablecimiento de las comunicaciones" (art. 197) del CP,[83] dotándolo de una amplitud comprensiva de los sistemas informáticos con relación al "entorpecimiento" como modalidad típica que guarda correspondencia con la "obstaculización grave".

Complementariamente, puede recordarse que por ley 25.891 —año 2004—, que regula los servicios móviles de telefonía y comunicación, se introdujeron los tipos de alteración, reemplazo, duplicación o modificación de número de línea o de serie electrónico o mecánico de un equipo terminal o de un módulo de identificación removible (MIR) en equipos terminales provistos; de modo que pueda ocasionar perjuicio al titular o usuario del terminal celular o terceros (art. 10), e idéntica conducta respecto de tarjeta de telefonía o el acceso a los códigos informáticos de habilitación de créditos del servicio de comunicaciones móviles (SCM) para aprovecharse ilegítimamente (art. 11). También se tipifica la adquisición o uso a sabiendas de la procedencia ilegítima de terminales celulares, MIR o tecnología similar que la reemplace en el futuro (art. 12). Las conductas se agravan si fueron cometidas con ánimo de lucro o como medio para perpetrar otro delito (art. 13), o por dependientes de empresas licenciatarias de SCM o quien posee en el desempeño de sus funciones acceso a las facilidades técnicas de aquellas (art. 14).

a.2 **Brasil**: ha consagrado en el marco de la protección de los derechos del consumidor dos tipos penales relativos a la información almacenada de contenido privado. Se trata de los artículos 72 y 73 del Código de Defensa del Consumidor, ley 8079/90. El primero pune con detención de seis meses a un año o multa el impedir o dificultar el acceso del consumidor a las informaciones que constan en bancos de datos, fichas o registros, referentes a su persona, mientras que el segundo lo hace con detención de uno a seis meses o multa respecto de la omisión del agente que no procede a la corrección inmediata de la tal información del consumidor que sabe o debería saber inexacta.

Por ley 12.737, del 30 de noviembre de 2012, se modificó el artículo 266 (84) del CP. Se incluyó dentro de las tipicidades de interrupción o perturbación

(83) Dice: "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".

(84) Su texto: *"art. 266 - Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento: Pena - detenção, de um a três anos, e multa.*
§ 1º Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento.
§ 2º Aplicam-se as penas em dobro se o crime é cometido por ocasião de calamidade pública".

de servicio la que se brinda por medio telemático o de información de utilidad pública, o la que impida o dificulte su restablecimiento (parág. 1º).

a.3 **Colombia**: incorporó al CP la figura de obstaculización ilegítima de sistema informático o red de telecomunicación (art. 269B)[85] en el marco de reforma por ley 1273 del año 2009.

a.4 **Ecuador**: a partir de la reforma introducida por ley 2002-37 se agregó, a continuación del artículo 415 del CPE, un artículo sin número,[86] cuyo segundo segmento tipifica la conducta de alteración o inutilización de las instalaciones físicas necesarias para la transmisión, recepción o procesamiento de mensajes de datos. La interrupción o violenta resistencia al restablecimiento de las comunicaciones está contemplada en el artículo 422[87] del CPE.

a.5 **Paraguay**: la obstaculización en un procesamiento de datos de un particular, de una empresa, asociación o de una entidad de la administración pública; así como la destrucción, inutilización, sustracción o alteración de una instalación de procesamiento de datos, de una unidad de almacenamiento o de otra de sus partes componentes indispensable son contempladas en el tipo de sabotaje informático del artículo 175 del CP de 1997, ya transcripto. Por la reforma de 2011, ley 4439, junto al artículo 174, es delito de instancia privada (art. 175b).

a.6 **Perú**: la alteración, daño y destrucción de sistema, red o programa de computadoras se había incorporado al CP de 1991 por ley 27.309 del 17 de julio de 2000 (art. 207-B). Eran aplicables los agravantes del artículo 207-C. Fueron derogados por la "disposición complementaria derogatoria única" de la ley 30096 de 2013 sobre "Delitos informáticos", que prevé el "Atentado contra la integridad de sistemas informáticos" (art. 4º).[88]

(85) Dice: "El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor".

(86) Tiene la siguiente redacción: "art. ... (2). Si no se tratare de un delito mayor, la destrucción, alteración o inutilización de la infraestructura o instalaciones físicas necesarias para la transmisión, recepción o procesamiento de mensajes de datos, será reprimida con prisión de 8 meses a 4 años y multa de 200 a 600 dólares…".

(87) Su parte pertinente dice: "Será reprimido con prisión de seis meses a dos años el que interrumpiere la comunicación postal, telegráfica, telefónica, radiofónica o de otro sistema, o resistiere violentamente al restablecimiento de la comunicación interrumpida…"(art. 422).

(88) Su texto: "El que, a través de las tecnologías de la información o de la comunicación, inutiliza, total o parcialmente, un sistema informático, impide el acceso a este, entorpece o imposibilita su funcionamiento o la prestación de sus servicios, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días multa".

a.7 **Venezuela**: el artículo 6° de la LECDI, ya citado y transcripto porque tipifica una variada alternativa de conductas, pena la interferencia de sistema que utilice tecnologías de la información; además, el evocado artículo 7° sanciona la directa inutilización. Estas conductas también serían punibles a título culposo conforme la remisión que formula el artículo 8°. A su vez, el artículo 21 pena al que mediante el uso de las tecnologías de la información desvía cualquier mensaje de datos o señal de transmisión o comunicación ajena.

b. Por su lado, los restantes estados —**Bolivia, Chile y Uruguay**— no han sancionado figuras receptivas de la propuesta del Convenio.

2.5 | Abuso de equipos e instrumentos técnicos (art. 6)

"1. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, las siguientes conductas cuando éstas sean cometidas dolosamente y sin autorización:

a. la producción, venta, obtención para su utilización, importación, difusión u otras formas de puesta a disposición:

- de un dispositivo, incluido un programa informático, principalmente concebido o adaptado para permitir la comisión de una de las infracciones establecidas en los arts. 2 a 5 arriba citados;
- de una palabra de paso (contraseña), de un código de acceso o de datos informáticos similares que permitan acceder a todo o parte de un sistema informático, con la intención de utilizarlos como medio para cometer alguna de las infracciones previstas en los arts. 2 a 5; y

b. la posesión de alguno de los elementos descritos en los parágrafos (a) (1) o (2) con la intención de utilizarlos como medio para cometer alguna de las infracciones previstas en los arts. 2-5. Los Estados podrán exigir en su derecho interno que concurra un determinado número de elementos para que nazca responsabilidad penal.

2. Lo dispuesto en el presente artículo no generará responsabilidad penal cuando la producción, venta, obtención para la utilización, importación, difusión u otras formas de puesta a disposición mencionadas en el párr. 1 no persigan la comisión de una infracción prevista en los arts. 2 a 5 del presente Convenio, como en el caso de ensayos autorizados o de la protección de un sistema informático.

> 3. Las Partes podrán reservarse el derecho de no aplicar el párr. 1, a condición de que dicha reserva no recaiga sobre la venta, distribución o cualesquiera otras formas de puesta a disposición de los elementos mencionados en el parágrafo 1 (a)(2)".[89]

a. En este artículo el Convenio propone la tipificación de una etapa previa al uso con relación a los dispositivos concebidos o adaptados para permitir alguna de las conductas descriptas en los anteriores o de contraseñas, códigos de acceso o datos que lo permitan a todo o parte de un sistema informático: la de su producción, venta, obtención para su utilización, importación, difusión u otras formas de puesta a disposición.

También la simple posesión de aquellos elementos con intención de uso para cometer alguna de las infracciones de los arts. 2 a 5, aunque en este caso se indica posible limitación vía exigencia local de la concurrencia de un determinado número de elementos para que nazca responsabilidad penal. En particular, se trata de una directriz expansiva del Convenio que viene a postular la criminalización de la simple posesión de los llamados *hacking tools* u otro *software* peligroso, como resalta con acierto Anarte Borrallo, quien la menciona como ejemplo de lo que puede resultar en algún caso como producto de disfunciones en la tendencia armonizadora hacia un sistema de persecución universalizado.[90]

El parág. 2, tal vez redundante, deja afuera los casos en que no hay intención de cometer las infracciones descriptas ejemplificando con ensayos au-

(89) Si bien la DM del año 2005 no previó equivalente, su sustituta Directiva 2013/40/UE del Parlamento Europeo y del Consejo de 12 de agosto de 2013 relativa a los ataques contra los sistemas de información, ha reafirmado la propuesta típica en su artículo 7°, con un texto más económico que dice: "Los Estados miembros adoptarán las medidas necesarias para garantizar que la producción intencional, venta, adquisición para el uso, importación, distribución u otra forma de puesta a disposición de los siguientes instrumentos, sin autorización y con la intención de que sean utilizados con el fin de cometer cualquiera de las infracciones mencionadas en los arts. 3 a 6, sea sancionable como infracción penal, al menos en los casos que no sean de menor gravedad:

a) un programa informático, concebido o adaptado principalmente para cometer una infracción de las mencionadas en los arts. 3 a 6;

b) una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información".

(90) Anarte Borrallo, Enrique, "Incidencia de las nuevas tecnologías en el sistema penal. Aproximación al derecho penal en la sociedad de la información", en *Derecho y Conocimiento*, Servicio de Publicaciones de la Facultad de Derecho de la Universidad de Huelva, vol. 1, p. 214.

torizados o la protección de un sistema informático. A su vez, el parág. 3 contempla la posible reserva de aplicación del parág. 1; salvo en lo concerniente a la venta, distribución o cualquier otra forma de puesta a disposición de tales elementos.

En general, implica un adelantamiento de la intervención penal que constituiría la punición autónoma de actos preparatorios de las restantes tipicidades, lo que explica la amplitud de las posibles reservas que se describen.

b. El repaso normativo regional verifica tipos vinculados en:

b.1 **Argentina**: la reforma del artículo 183 del CP por ley 26.388 del año 2008 —ya transcripto—, introdujo, en su última parte, la punición de la venta, distribución, puesta en circulación o introducción en un sistema informático de cualquier programa destinado a causar daños.

En cambio, con directa vinculación con observación formulada en el punto anterior, Nora Cherñavsky destaca que no se ha tipificado la mera tenencia o posesión de códigos, contraseñas u otros datos que permitan acceder a un sistema informático en relación con la posible lesión a la integridad y confidencialidad de los mismos, incriminación de peligro abstracto prevista en el inc. b del artículo 6° antes transcripto.(91)

b.2 **Brasil**: en su Ley Electoral N° 9100 —año 1995—, prevé reclusión de tres a seis años y multa para quien intente desarrollar o introducir un comando, instrucción o programa de computación capaz de destruir, apagar, eliminar, alterar, grabar o transmitir dato, instrucción o programa o provocar cualquier otro resultado diverso del esperado en el sistema de tratamiento automatizado de datos utilizado por el sistema electoral (art. 67, inc. VIII).

Más reciente es la modificación del artículo 154-A del CP por ley 12.737 —año 2012— que, entre otras conductas base, prevé la de instalar vulnerabilidades para obtener una ventaja ilícita y, con idéntica pena —detención de 3 meses a un año y multa—, para el que produzca, ofrezca, distribuya, venda o difunda dispositivo o programa de computación con el propósito de permitir alguna de las conductas anteriores (parág. 1º). Se agrava la pena de un sexto a un tercio si resulta perjuicio económico (parág. 2º). También se agrava, pero de un tercio a la mitad, si el delito es practicado contra los más altos funcionarios de los poderes del Estado.

b.3 **Colombia**: la indicada modificación al CP del año 2009 por ley 1273 incluyó un tipo de "uso de software malicioso" como artículo 269E.(92)

(91) Cherñavsky, *op. cit.*, pp. 284/285.

(92) Su redacción: "El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros

b.4 **Paraguay**: mediante la ley 4439 —año 2011— se incorporó al Código Penal la preparación de acceso indebido e interceptación de datos (art. 146d).[93]

b.5 **Perú**: con su nueva ley 30.096 de 2013 ha incorporado un tipo específico correspondiente en su capítulo VII —"Disposiciones comunes"—, artículo 10 —"Abuso de mecanismos y dispositivos informáticos"—.[94] A su vez, aplicable a todas las figuras de la ley especial, el artículo 11[95] prevé los "Agravantes" de orden genérico que, según se podrá advertir de una lectura integral, en muchos casos aparece como redundante, en la medida que las circunstancias de agravación ya han sido incorporadas expresamente en algunas de las figuras que le preceden.

b.6 **Venezuela**: pune mediante el artículo 10[96] de su LECDI —año 2001— la "Posesión de equipos o prestación de servicios de sabotaje".

programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes".

(93) Su texto: "Artículo 146 d. Preparación de acceso indebido e interceptación de datos. 1° El que prepare un hecho punible según el art. 146 b o el art. 146 c produciendo, difundiendo o haciendo accesible de otra manera a terceros: 1) las claves de acceso u otros códigos de seguridad, que permitan el acceso a datos en sentido del art. 146 b, inc. 2; o 2) los programas de computación destinados a la realización de tal hecho, será castigado con pena privativa de libertad de hasta un año o multa. 2° Se aplicará, en lo pertinente, lo previsto en el art. 266, incs. 2 y 3".

(94) Dice: "El que fabrica, diseña, desarrolla, vende, facilita, distribuye, importa u obtiene para su utilización uno o más mecanismos, programas informáticos, dispositivos, contraseñas, códigos de acceso o cualquier otro dato informático, específicamente diseñados para la comisión de los delitos previstos en la presente Ley, o el que ofrece o presta servicio que contribuya a ese propósito, será reprimido con una pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días multa".

(95) Su redacción: "El juez aumentará la pena privativa de libertad hasta en un tercio por encima del máximo legal fijado para cualquiera de los delitos previstos en la presente ley cuando:

1. El agente comete el delito en calidad de integrante de una organización criminal.
2. El agente comete el delito mediante el abuso de una posición especial de acceso a la data o información reservada o al conocimiento de esta información en razón del ejercicio de un cargo o función.
3. El agente comete el delito con el fin de obtener un beneficio económico, salvo en los delitos que prevén dicha circunstancia.
4. El delito compromete fines asistenciales, la defensa, la seguridad y la soberanía nacionales".

(96) Su texto: "Quien importe, fabrique, distribuya, venda o utilice equipos, dispositivos o programas, con el propósito de destinarlos a vulnerar o eliminar la seguridad de cualquier sistema que utilice tecnologías de la información; o el que ofrezca o preste servicios destinados a cumplir los mismos fines, será penado con prisión de tres a seis años y multa de trescientas a seiscientas unidades tributarias".

c. En los restantes estados bajo comparación —**Bolivia, Chile, Ecuador** y **Uruguay**—, no se advierten figuras penales específicas vigentes que aprehendan la propuesta de Budapest.

3 | Las infracciones informáticas

El Título II de la Sección 1 —"Infracciones informáticas"—, se compone de dos artículos mediante los que se indica la necesidad de tipificar la falsedad y la estafa informáticas, del siguiente modo:

3.1 | Falsedad informática (art. 7)

> "Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, la introducción, alteración, borrado o supresión dolosa y sin autorización de datos informáticos, generando datos no auténticos, con la intención de que sean percibidos o utilizados a efectos legales como auténticos, con independencia de que sean directamente legibles e inteligibles. Las Partes podrán reservarse el derecho a exigir la concurrencia de un ánimo fraudulento o de cualquier otro ánimo similar para que nazca responsabilidad penal".

a. La generación de datos falsos —sean o no directamente legibles— con intención de que a los efectos legales fueren percibidos o utilizados como auténticos, admite como limitación para los estados signatarios la de exigir en su derecho interno la concurrencia de ánimo de fraude.

b. Puede advertirse en este caso que, tipos o figuras penales locales que fueron individualizados al tratar los atentados a la integridad de datos, brindan parcial cobertura a esta tipicidad. Además, la posible exigencia de intención fraudulenta conduciría muchos otros casos al ámbito de los fraudes informáticos. Ésto dificulta el hallazgo de figuras expresas que reproduzcan la descripción básica del Convenio sin que, sin embargo, pueda considerarse que existen "vacíos" o "lagunas" de punición locales. Así, por ejemplo, la confluencia entre la regulación que protege la integridad de datos personales y la que pune las defraudaciones, permi-

tiría evitar lo que, a primera vista, luciría como atípico por no haber una regla especial que reproduzca con similar terminología el artículo 7 del Convenio. Sentado ello, pueden encontrarse otras normas que guardan vinculación y que no han sido incluidas en ninguno de los acápites mencionados en:

b.1 **Argentina**: ha modificado su regulación de las falsedades documentales. Primero, por vía de la LPDP del año 2000. Luego, por la ley 26.388 del año 2008, incorporó tres nuevos párrafos finales en la parte general al artículo 77[97] del CP, en los que se define al documento y la firma digital. Se provocó con ello una suerte de efecto cascada que amplificó todas las referencias de los tipos de la parte especial.

b.2 **Brasil**: en materia de falsedades, por ley 12.737 del 30 de noviembre de 2012, se modificó el tipo de la falsificación de documento particular (art. 298 del CP), que prevé pena de reclusión de uno a cinco años y multa, e incluye equiparadamente las tarjetas de crédito o débito.

b.3 **Chile**: por artículo 5[98] de la ley 20.009 del 1° de abril de 2005, se introdujeron al derecho chileno varios tipos penales relativos al uso de tarjetas de crédito y débito y a las claves asociadas como modalidades de fraude, por lo que se lo verá en perspectiva del artículo 8° del Convenio.

(97) Con el siguiente texto: "…El término documento comprende toda representación de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión. Los términos firma y suscripción comprenden la firma digital, la creación de una firma digital o firmar digitalmente. Los términos instrumento privado y certificado comprenden el documento digital firmado digitalmente".

(98) Dice: "Artículo 5°. Las siguientes conductas constituyen delito de uso fraudulento de tarjeta de crédito o débito:

a) Falsificar tarjetas de crédito o débito.

b) Usar, vender, exportar, importar o distribuir tarjetas de crédito o débito falsificadas o sustraídas.

c) Negociar, en cualquier forma, con tarjetas de crédito o débito falsificadas o sustraídas.

d) Usar, vender, exportar, importar o distribuir los datos o el número de una tarjeta de crédito o débito, haciendo posible que terceros realicen operaciones de compra o de acceso al crédito o al débito que corresponden exclusivamente al titular.

e) Negociar, en cualquier forma, con los datos o el número de la tarjeta de crédito o débito, para las operaciones señaladas en la letra anterior.

f) Usar maliciosamente una tarjeta bloqueada, en cualquiera de las formas señaladas en las letras precedentes.

La pena por este delito será de presidio menor en cualquiera de sus grados. Esta pena se aplicará en su grado máximo, si la acción realizada produce perjuicio a terceros".

b.4 **Paraguay**: ha incorporado por ley 4439 del año 2011, un tipo que pune la falsificación o alteración de tarjetas de crédito o de débito o cualquier otro medio electrónico de pago (art. 248b).[99] Se incluye también su adquisición para sí o para tercero, el ofrecimiento, la entrega a otro o el uso de esas tarjetas o medio electrónico de pago.

b.5 **Uruguay**: por ley 16.002 del 25 de octubre de 2088, introdujo los delitos que punen la falsificación documentaria en casos de transmisión a distancia por medios electrónicos (arts. 129[100] y 130),[101] con remisión a los artículos 236 a 239[102] del CP, que se refieren a los documentos públicos. Luego, por

(99) Con la siguiente redacción: "Artículo 248 b. Falsificación de tarjetas de débito o de crédito y otros medios electrónicos de pago. 1° El que, con la intención de inducir en las relaciones jurídicas al error o de facilitar la inducción a tal error: 1) falsificare o alterare una tarjeta de crédito o débito u otro medio electrónico de pago; o 2) adquiera para sí o para un tercero, ofreciere, entregare a otro o utilizare tales tarjetas o medios electrónicos, será castigado con pena privativa de libertad de hasta cinco años o con multa. 2° Se castigará también la tentativa. 3° Cuando el autor actuara comercialmente o como miembro de una organización criminal dedicada a la realización de los hechos punibles señalados, la pena privativa de libertad podrá ser aumentada hasta diez años. 4° Tarjetas de crédito, en sentido del inc. 1, son aquellas que han sido emitidas por una entidad de crédito o de servicios financieros para su uso en dicho tipo de transacciones y que, por su configuración o codificación, son especialmente protegidas contra su falsificación. 5° Medios electrónicos de pago en el sentido del inc. 1, son aquellos instrumentos o dispositivos que actúan como dinero electrónico, permitiendo al titular efectuar transferencias de fondos, retirar dinero en efectivo, pagar en entidades comerciales y acceder a los fondos de una cuenta".

(100) Dice: "La documentación emergente de la transmisión a distancia, por medios electrónicos, entre dependencias oficiales, constituirá, de por sí, documentación auténtica y hará plena fe a todos sus efectos en cuanto a la existencia del original trasmitido".

(101) Su texto: "El que voluntariamente trasmitiere a distancias entre dependencias oficiales un texto del que resulte un documento infiel, incurrirá en los delitos previstos por los arts. 236 a 239 del Código Penal, según corresponda".

(102) Sus textos: 236. (Falsificación material en documento público, por funcionario público). El funcionario público que ejerciendo un acto de su función, hiciere un documento falso o alterare un documento verdadero, será castigado con tres a diez años de penitenciaría. Quedan asimilados a los documentos, las copias de los documentos inexistentes y las copias infieles de documento existente.

237. (Falsificación o alteración de un documento público, por un particular o por un funcionario, fuera del ejercicio de sus funciones). El particular o funcionario público que fuera del ejercicio de sus funciones, hiciere un documento público falso o alterare un documento público verdadero, será castigado con dos a seis años de penitenciaría.

238. (Falsificación ideológica por un funcionario público). El funcionario público que, en el ejercicio de sus funciones, diere fe de la ocurrencia de hechos imaginarios o de hechos reales, pero alterando las circunstancias o con omisión o modificación de las declaraciones prestadas con ese motivo o mediante supresión de tales declaraciones, será castigado con dos a ocho años de penitenciaría.

ley 18.600 de documento electrónico y firma digital —del 21 de septiembre de 2009—, estableció un tipo de mayor especificidad (art. 4, inc. 2).[103]

b.6 **Venezuela**: También tipifica las falsificaciones documentales en su LECDI de 2001 (art. 12)[104] y, además, la posesión de equipos destinados a falsificar tarjetas inteligentes o instrumentos análogos (art. 19).[105]

c. Los estados regionales que carecen de tipo específico y que no cubrirían el vacío en la forma indicada en el precedente primer párrafo "b" serían Bolivia, Colombia, Ecuador y Perú. En este último caso, la nueva ley 30.096 de 2013, en el capítulo VI —dedicado a los "Delitos Informáticos contra la Fe Pública"—, sólo prevé la figura de "suplantación de identidad" en el único artículo que lo integra (art. 9°).[106]

3.2 | Estafa informática (art. 8)

"Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal,

239. (Falsificación ideológica por un particular). El que, con motivo del otorgamiento o formalización de un documento público, ante un funcionario público, prestare una declaración falsa sobre su identidad o estado, o cualquiera otra circunstancia de hecho, será castigado con tres a veinticuatro meses de prisión.

(103) Su redacción es la siguiente: "El que voluntariamente transmitiere un texto del que resulte un documento infiel, adultere o destruya un documento almacenado en soporte magnético, o su respaldo, incurrirá en los delitos previstos por los arts. 236 a 239 del CP, según corresponda".

(104) Dice: "Falsificación de documentos. Quien, a través de cualquier medio, cree, modifique o elimine un documento que se encuentre incorporado a un sistema que utilice tecnologías de información; o cree, modifique o elimine datos del mismo; o incorpore a dicho sistema un documento inexistente, será penado con prisión de tres a seis años y multa de trescientas a seiscientas unidades tributarias. Cuando el agente hubiere actuado con el fin de procurar para sí o para otro algún tipo de beneficio, la pena se aumentará entre un tercio y la mitad.
El aumento será de la mitad a dos tercios si del hecho resultare un perjuicio para otro".

(105) Su texto: "Posesión de equipo para falsificaciones. Todo aquel que sin estar debidamente autorizado para emitir, fabricar o distribuir tarjetas inteligentes o instrumentos análogos, reciba, adquiera, posea, transfiera, comercialice, distribuya, venda, controle o custodie cualquier equipo de fabricación de tarjetas inteligentes o los instrumentos destinados a los mismos fines, o cualquier otro equipo o componente que capture, grabe, copie o transmita la data o información de dichas tarjetas o instrumentos, será penado con prisión de tres a seis años y multa de trescientas a seiscientas unidades tributarias".

(106) Dice: "El que, mediante las tecnologías de la información o de la comunicación suplanta la identidad de una persona natural o jurídica, siempre que de dicha conducta resulte algún perjuicio, material o moral, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años".

conforme a su derecho interno, 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,
- 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 tercero".

a. Se trata de una de las previsiones del Convenio que ha recibido críticas de la doctrina, en vistas a que no proporciona una definición de estafa ni brinda una respuesta clara a la utilización abusiva de tarjetas.[107] Con relación a ella se encuentran normas receptivas en los siguientes estados:

a.1 **Argentina**: introdujo dos reformas al CP que consistieron en el agregado de incisos al artículo 173, que ya preveía 14 modalidades de estafas y fraudes pero no vinculadas a las nuevas tecnologías. Por ley 25.930 —año 2004— se incorporó el inc. 15,[108] vinculado a las tarjetas; mientras que por ley 26.388 —año 2008— se agregó el 16.[109] La pena, por remisión al artículo 172, es de un mes a seis años de prisión.

a.2 **Bolivia**: el artículo 363*bis*[110] del CP —año1997—, bajo la designación de "Manipulación informática", es el que cubre el reclamo de tipicidad.

a.3 **Chile**: por el ya transcripto artículo 5° de la ley 20.009, del 1° de abril de 2005, se introdujo varios tipos penales relativos al uso de tarjetas de crédito y débito y a las claves asociadas.

a.4 **Colombia**: en el marco del capítulo II del nuevo Título incorporado al CP por ley 1273 —año 2009—, se prevén las conductas de "hurto por medios

(107) García-Cervigón, Josefina, "El fraude informático en España e Italia. Tratamiento jurídico-penal y criminológico", en *ICADE. Revista cuatrimestral de las Facultades de Derecho y Ciencias Económicas y Empresariales*, UNED, n° 74, mayo-agosto 2008, p. 291 y Hirsh, *op. cit.*

(108) Dice: "15) El que defraudare mediante el uso de una tarjeta de compra, crédito o débito, cuando la misma hubiere sido falsificada, adulterada, robada, perdida u obtenida del legítimo emisor mediante ardid o engaño, o mediante el uso no autorizado de sus datos, aunque lo hiciese por medio de una operación automática".

(109) Su 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".

(110) Con esta redacción: "El que con la intención de obtener un beneficio indebido para sí o un tercero, manipule un procesamiento o transferencia de datos informáticos que conduzca a un resultado incorrecto o evite un proceso tal cuyo resultado habría sido correcto, ocasionando de esta manera una transferencia patrimonial en perjuicio de tercero. Sanción: reclusión de 1 a 5 años y multa de 60 a 200 días".

informáticos y semejantes" (art. 269-I)[111] y de "transferencia no consentida de activos" (art. 269-J).[112]

a.5 **Ecuador**: por ley 2002-67 se introdujo —a continuación del artículo sobre conductas asimiladas al robo (art. 553 CPE)— un artículo sin número[113] con dos segmentos. El primero, dedicado a la apropiación ilícita a través del uso fraudulento de sistemas de información o redes electrónicas. El segundo, precisando las circunstancias agravantes. Además, en materia de conductas fraudulentas, se indica una consideración agravada por su perpetración usando medios electrónicos o telemáticos (art. 563).[114]

(111) Su texto: "El que, superando medidas de seguridad informáticas, realice la conducta señalada en el art. 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el art. 240 de este Código".

(112) Dice: "El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1500 salarios mínimos legales mensuales vigentes. La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa.

Si la conducta descrita en los dos incisos anteriores tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad".

(113) Dice: art. ... (1). (Ag. por art. 62, L. 2002-67, R.O. 557-S, 17-IV-2002). Apropiación ilícita. Serán reprimidos con prisión de seis meses a cinco años y multa de quinientos a mil dólares de los EU de N, los que utilizaren fraudulentamente sistemas de información o redes electrónicas, para facilitar la apropiación de un bien ajeno, o los que procuren la transferencia no consentida de bienes, valores o derechos de una persona, en perjuicio de ésta o de un tercero, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas informáticos, sistemas informáticos, telemáticos o mensajes de datos.
art. ... (2). (Ag. por art. 62, L. 2002-67, R.O. 557-S, 17-IV-2002). La pena de prisión de uno a cinco años y multa de mil a dos mil dólares de los EUN, si el delito se hubiere cometido empleando los sigs. medios:

1. Inutilización de sistemas de alarma o guarda;
2. Descubrimiento o descifrado de claves secretas o encriptadas;
3. Utilización de tarjetas magnéticas o perforadas;
4. Utilización de controles o instrumentos de apertura a distancia; y,
5. Violación de seguridades electrónicas, informáticas u otras semejantes".

(114) Su texto: "art. 563 (inc. 2. Ag. por art. 63, L. 2002-67, R.O. 557-S, 17-IV-2002, ref. por art. 159, L. 2002-75, R.O. 635, 7-VIII-2002 y el último inc. ag. por art. 3, L. 2002-91, R.O. 716, 2-XII-2002). El que, con propósito de apropiarse de una cosa perteneciente a otro, se hubiere hecho entregar fondos, muebles, obligaciones, finiquitos, recibos, ya haciendo uso de nombres falsos, o de falsas calidades, ya empleando manejos fraudulentos para hacer creer en la existencia de falsas empresas, de un poder, o de un crédito imaginario, para infundir la

a.6 **Paraguay**: el nuevo Código Penal ha introducido en su capítulo dedicado a los delitos contra el patrimonio dos tipos específicos vinculados. Uno, de operaciones fraudulentas por computadora (art. 188);[115] y otro, de aprovechamiento clandestino de una prestación (art. 189).[116] El primero ha sido modificado por la ley 4439 del 5 de octubre de 2011, que la rebautizó como "Estafa mediante sistemas informáticos".

a.7 **Perú**: su regulación sobre las estafas era genérica. A partir de la modificación del CP —año 1991— por ley 29.316 del 14 de enero de 2009 protegía las señales satelitales portadoras de programas; puniendo tanto la cadena que va desde la fabricación hasta la distribución de dispositivos para asistir a la decodificación (art. 186-A), como hasta la distribución

esperanza o el temor de un suceso, accidente, o cualquier otro acontecimiento quimérico, o para abusar de otro modo de la confianza o de la credulidad, será reprimido con prisión de seis meses a cinco años y multa de ocho a ciento cincuenta y seis dólares de los Estados Unidos de Norte América.
Será sancionado con el máximo de la pena prevista en el inciso anterior y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica, el que cometiere el delito utilizando medios electrónicos o telemáticos.
La pena será de reclusión menor ordinaria de tres a seis años, si la defraudación se cometiera en casos de migraciones ilegales".

(115) Su texto: "Art. 188. Estafa mediante sistemas informáticos.
1° El que, con la intención de obtener para sí o para un tercero un beneficio patrimonial indebido, influyera sobre el resultado de un procesamiento de datos mediante:

1) una programación incorrecta;

2) el uso de datos falsos o incompletos;

3) el uso indebido de datos; u

4) la utilización de otra maniobra no autorizada; y con ello causara un perjuicio al patrimonio de otro, será castigado con pena privativa de libertad de hasta cinco años o con multa.

2° En estos casos, se aplicará también lo dispuesto en el art. 187, incs. 2 al 4.

3° El que preparare un hecho punible señalado en el inc. 1, mediante la producción, obtención, venta, almacenamiento u otorgamiento a terceros de programas de computación destinados a la realización de tales hechos, será castigado con pena privativa de libertad de hasta tres años o con multa.

4° En los casos señalados en el inc. 3, se aplicará lo dispuesto en el art. 266, incs. 2 y 3".

(116) Dice: "Artículo 189. Aprovechamiento clandestino de una prestación.

1° El que con la intención de evitar el pago de la prestación, clandestinamente:

1) se aprovechara del servicio de un aparato automático, de una red de telecomunicaciones destinada al público, o de un medio de transporte; o

2) accediera a un evento o a una instalación, será castigado con pena privativa de libertad de hasta un año o con multa, siempre que no estén previstas penas mayores en otro artículo.

2° En estos casos, será castigada también la tentativa.

3° En lo pertinente se aplicará lo dispuesto en los arts. 171 y 172".

misma de señales (art. 194-A).[117] El artículo 186-A citado ha sido derogado por la nueva ley 30.096 de 2013 —no así el 194-A—, por vía de su disposición complementaria derogatoria única. A su vez, en su capítulo V —"Delitos informáticos contra el patrimonio"—, dedica al "Fraude informático" (art. 8°) su único artículo.[118]

a.8 **Venezuela**: su LECDI dedica el capítulo II a los "Delitos contra la Propiedad", donde se prevén tipos especiales de fraude (art. 14),[119] obtención indebida de bienes o servicios (art. 15),[120] manejo fraudulento de tarjetas inteligentes o instrumentos análogos (art. 16),[121] apropiación de tarjetas

(117) Su texto: "Artículo 194-A. Distribución de señales de satélite portadoras de programas. El que distribuya una señal de satélite portadora de programas, originariamente codificada, a sabiendas que fue decodificada sin la autorización del distribuidor legal de dicha señal, será reprimido con pena privativa de la libertad no menor de dos años ni mayor de seis años y con treinta a noventa días multa".

(118) Su texto: "El que, a través de las tecnologías de la información o de la comunicación, procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, será reprimido con una pena privativa de libertad no menor de tres ni mayor de ocho años y con sesenta a ciento veinte días multa.

La pena será privativa de libertad no menor de cinco ni mayor de diez años y de ochenta a ciento cuarenta días multa cuando se afecte el patrimonio del Estado destinado a fines asistenciales o a programas de apoyo social".

(119) Sería el tipo básico. Dice: "Fraude. Todo aquel que, a través del uso indebido de tecnologías de información, valiéndose de cualquier manipulación en sistemas o cualquiera de sus componentes, o en la data o información en ellos contenida, consiga insertar instrucciones falsas o fraudulentas, que produzcan un resultado que permita obtener un provecho injusto en perjuicio ajeno, será penado con prisión de tres a siete años y multa de trescientas a setecientas unidades tributarias".

(120) Dice: "Obtención indebida de bienes o servicios. Quien, sin autorización para portarlos, utilice una tarjeta inteligente ajena o instrumento destinado a los mismos fines, o el que utilice indebidamente tecnologías de la información para requerir la obtención de cualquier efecto, bien o servicio; o para proveer su pago sin erogar o asumir el compromiso de pago de la contraprestación debida, será castigado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias".

(121) Su redacción: "Manejo fraudulento de tarjetas inteligentes o instrumentos análogos. Toda persona que por cualquier medio cree, capture, grabe, copie, altere, duplique o elimine la data o información contenidas en una tarjeta inteligente o en cualquier instrumento destinado a los mismos fines; o la persona que, mediante cualquier uso indebido de tecnologías de información, cree, capture, duplique o altere la data o información en un sistema, con el objeto de incorporar usuarios, cuentas, registros o consumos inexistentes o modifique la cuantía de estos, será penada con prisión de cinco a diez años y multa de quinientas a mil unidades tributarias.
En la misma pena incurrirá quien, sin haber tomado parte en los hechos anteriores, adquiera, comercialice, posea, distribuya, venda o realice cualquier tipo de intermediación de tarjetas

inteligentes o instrumentos análogos (art. 17)[122] y provisión indebida de bienes o servicios (art. 18).[123]

b. Aunque en términos estrictos no implique que sean casos de atipicidad sino que se subsumen en tipos clásicos, puede advertirse la carencia de normas específicas en:

b.1 **Brasil**: su situación es la de disputa doctrinaria; similar a la de Argentina previo a la ley 26.388, descripta anteriormente. Al mantenerse la redacción histórica de la estafa, se discute si se trata de una modalidad de aquella o de un hurto. Hay un tipo vinculado al fraude fiscal. Por ley 8137 del 27 de diciembre de 1990, sobre "Crímenes contra el orden económico y las relaciones de consumo", se establece una nueva forma de uso ilícito del ordenador definida como la acción de utilizar o divulgar programas de procesamiento de datos que permitan al contribuyente poseer información contable diversa a la que es, por ley, proporcionada a la Hacienda Pública. Tiene pena de detención de 6 meses a 2 años y multa.

b.2 **Uruguay**: introdujo como actualización normativa la penalización del uso indebido de señales destinadas a ser recibidas en régimen de suscripción por ley 17.520 del 19 de julio de 2002, puniendo la captación (art. 1°)[124] y el efectuarla a favor de tercero (art. 2°),[125] con distintas agravan-

inteligentes o instrumentos destinados al mismo fin, o de la data o información contenidas en ellos o en un sistema".

(122) Su texto: "Apropiación de tarjetas inteligentes o instrumentos análogos. Quien se apropie de una tarjeta inteligente o instrumento destinado a los mismos fines, que se haya perdido, extraviado o que haya sido entregado por equivocación, con el fin de retenerlo, usarlo, venderlo o transferirlo a una persona distinta del usuario autorizado o entidad emisora, será penado con prisión de uno a cinco años y multa de diez a cincuenta unidades tributarias.
La misma pena se impondrá a quien adquiera o reciba la tarjeta o instrumento a que se refiere el presente artículo".

(123) Dice: "Provisión indebida de bienes o servicios. Todo aquel que, a sabiendas de que una tarjeta inteligente o instrumento destinado a los mismos fines, se encuentra vencido, revocado; se haya indebidamente obtenido, retenido, falsificado, alterado; provea a quien los presente de dinero, efectos, bienes o servicios, o cualquier otra cosa de valor económico será penado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias".

(124) Su redacción: "El que, para provecho propio o de un tercero, captare señales trasmitidas por cualquier medio destinadas exclusivamente a ser recibidas en régimen de abonados, sin serlo, será castigado con 80 UR (ochenta unidades reajustables) a 800 UR (ochocientas unidades reajustables), de multa o prisión equivalente".

(125) Dice: "El que, con o sin ánimo de lucro, efectuare a favor de un tercero, las instalaciones, manipulaciones, o cualquier otra actividad necesaria para la obtención de los hechos que determinan la conducta típica descrita en el artículo anterior, será castigado con pena de tres meses de prisión a tres años de penitenciaría".

tes (art. 3°);[126] así como también conductas favorecedoras relacionadas con los aparatos de decodificación o similares (art. 4°).[127]

4 | Infracciones relativas al contenido

4.1 | Infracciones relativas a la pornografía infantil (art. 9)

En el Título 3 —"Infracciones relativas al contenido"— se prevé un solo artículo, "Infracciones relativas a la pornografía infantil" (art. 9°), que incluye una serie de conductas que propone tipificar y conceptos que precisan lo que serían para nosotros elementos normativos del tipo. En este sentido, el texto dice:

> "1. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, las siguientes conductas cuando éstas sean cometidas dolosamente y sin autorización:
>
> - la producción de pornografía infantil con la intención de difundirla a través de un sistema informático;
> - el ofrecimiento o la puesta a disposición de pornografía infantil a través de un sistema informático;
> - la difusión o la transmisión de pornografía infantil a través de un sistema informático;
> - el hecho de procurarse o de procurar a otro pornografía infantil a través de un sistema informático;

(126) Con esta redacción: "Las penas de los delitos anteriores serán aumentadas de un tercio a la mitad:

1) Si las conductas se realizaren mediante la producción de un daño a la red, instalaciones conexas, equipos o cualquier otro elemento técnico pertenecientes a la empresa autorizada prestadora del servicio, cualquiera sea el lugar que ellos estuvieran colocados.
2) Si las conductas ocasionaren una interrupción o perturbación del servicio o un menoscabo efectivo de su calidad, en perjuicio de otros suscriptores.
3) Cuando el agente revista la calidad de empleado, ex-empleado o arrendador de servicios de la empresa permisaria o del instalador autorizado".

(127) Su texto: "El que fabrique, importe, venda u ofrezca en venta, arriende o ponga en circulación decodificadores o cualquier otro artefacto, equipo o sistema diseñado exclusivamente para eliminar, impedir, desactivar o eludir los dispositivos técnicos que los titulares autorizados de la señal hayan instalado, para su protección, será castigado con pena de tres a veinticuatro meses de prisión".

- la posesión de pornografía infantil en un sistema informático o en un medio de almacenamiento de datos informáticos.

2. A los efectos del párrafo 1 arriba descrito, la "pornografía infantil" comprende cualquier material pornográfico que represente de manera visual:

- un menor adoptando un comportamiento sexualmente explícito;
- una persona que aparece como un menor adoptando un comportamiento sexualmente explícito;
- unas imágenes realistas que representen un menor adoptando un comportamiento sexualmente explícito.

3. A los efectos del párrafo 2 arriba descrito, el término "menor" designa cualquier persona menor de 18 años. Las Partes podrán exigir un límite de edad inferior, que debe ser como mínimo de 16 años.

4. Los Estados podrán reservarse el derecho de no aplicar, en todo o en parte, los párrafos 1 (d) y 1 (e) y 2 (b) y 2 (c)".[128]

a. En relación con la pornografía, la propuesta del Convenio limita la intervención penal a los casos que compromete a menores; por lo que, desde esta perspectiva, la conflictividad con los ordenamientos locales, en principio, no existe. La salvedad corresponde, en general, porque resulta inevitable la verificación de discrepancias al momento de interpretar los alcances de un elemento normativo teñido fuertemente por condicionantes culturales, como qué es "pornografía" u "obscenidad". Y, en particular, porque resulta inevitable la verificación de discrepancias al momento de la punición de casos en los que efectivamente no hay intervención de menores en el material pornográfico, sino de personas que aparecen como menores; o se trata de imágenes realistas que representan a un

(128) Rovira del Canto recuerda que la propuesta fue reafirmada mediante la DM 2004/68/JAI del Consejo, de 22 de diciembre de 2003, relativa a la lucha contra la explotación sexual de los niños y la pornografía infantil, cuyo art. 2 indica que los Estados miembros del Consejo adoptarán las medidas necesarias para la punibilidad como infracciones relacionadas con la explotación sexual de los niños, de las conductas intencionales siguientes: "a) coaccionar a un niño para que se prostituya o participe en espectáculos pornográficos, o lucrase con ello o explotar de cualquier otra manera a un niño para tales fines; b) captar a un niño para que se prostituya o participe en espectáculos pornográficos; d) practicar con un niño actividades sexuales recurriendo a algunos de los medios siguientes: i) hacer uso de la coacción, la fuerza o la amenaza; ii) ofrecer al niño dinero u otras formas de remuneración o de atenciones a cambio de que se preste a practicar actividades sexuales; iii) abusar de una posición de reconocida confianza, autoridad o influencia sobre el niño" (Rovira del Canto, *op. cit.*, p. 6).

menor (incs. 2.b y 2.c). De lo contrario, quedarían comprendidos casos de imágenes puramente virtuales sin ninguna base real.

Para muchos estados que han firmado el "Protocolo facultativo de la Convención sobre los derechos del niño relativo a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía" (Asamblea General de Naciones Unidas, sesión plenaria del 25 de mayo de 2000); el concepto de **pornografía infantil**, en concordancia con la previsión de Budapest que ahora nos ocupa, es "toda representación, por cualquier medio, de un niño dedicado a actividades sexuales explícitas, reales o simuladas, o todo representación de las partes genitales de un niño con fines primordialmente sexuales" (art. 2° inc. c).

Tanto en la región de Argentina como Brasil, luego de la primera aproximación —año 2003— en la discusión parlamentaria de sus respectivas leyes modificatorias internas, se optó por excluir las meras simulaciones de los tipos penales por su conflictividad constitucional; ya sea por contraposición con la libertad de expresión —representaciones artísticas, por ejemplo— o por posible derecho penal de autor —punición de la tendencia pederasta—. No obstante, se trata conforme el inc. 4° del Convenio, de dos de los casos en que los estados pueden formular reserva —los otros son el procurarse o procurarle a otro, y la simple posesión de material prohibido—. Corresponde aclarar que, en su segunda reforma del año 2008, en Brasil, se cambió de posición e incluyó la pornografía "virtual" y también la simple tenencia de imágenes como las referidas.

b. Una vez escrutadas las legislaciones nacionales de la región, se encuentran tipos específicos en:

b.1 **Argentina**: por la ley 26.388 —año 2008— se modificó el CP con la actualización del art. 128.[129] Debe tenerse presente que el citado "Protocolo faculta-

(129) El texto vigente reza: "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".

tivo…" ha sido incorporado a nuestro derecho interno por ley 25.763 —año 2003—, sin perjuicio de lo cual las actividades "simuladas" fueron excluidas. También lo ha sido la simple posesión, bajo consideración de tratarse de un tipo que merece un debate amplio que, por un lado, conlleva el problema de la polémica acerca de su posible incursión en ámbitos de reserva de moral sexual en equiparación con otras conductas mucho más graves y de directa lesividad y, por otro, no difiere demasiado del genérico alrededor de las figuras de "tenencia" punibles y los delitos de peligro abstracto.

b.2 **Brasil**: el Estatuto del Menor y del Adolescente (ECA, *Estatuto da Criança e Adolescente*, ley 8069/90) tipifica la conducta ampliando el crimen de "pornografía infantil" desde la reforma del art. 241 —12 de noviembre de 2003— por ley 10.764. En 2008, el ECA fue masiva y nuevamente modificado en sus previsiones penales por ley 11.829/08, con la intención de actualizarlo en el tema pedofilia.

Al presente, las normas de interés en la materia que nos ocupa son los arts. 240,[130] 241,[131] 241-A,[132] cuyo parág. 2° incluye la responsabilidad del ISP que debidamente notificado no deshabilita el acceso al contenido;

(130) Su texto: *"Produzir, reproduzir, dirigir, fotografar, filmar ou registrar, por qualquer meio, cena de sexo explícito ou pornográfica, envolvendo criança ou adolescente. Pena – reclusão, de 4 (quatro) a 8 (oito) anos, e multa.*
§ 1 Incorre nas mesmas penas quem agencia, facilita, recruta, coage, ou de qualquer modo intermedeia a participação de criança ou adolescente nas cenas referidas no caput deste artigo, ou ainda quem com esses contraseña.
§ 2 Aumenta-se a pena de 1/3 (um terço) se o agente comete o crime:
I – no exercício de cargo ou função pública ou a pretexto de exercê-la;
II – prevalecendo-se de relações domésticas, de coabitação ou de hospitalidade; ou
III – prevalecendo-se de relações de parentesco consangüíneo ou afim até o terceiro grau, ou por adoção, de tutor, curador, preceptor, empregador da vítima ou de quem, a qualquer outro título, tenha autoridade sobre ela, ou com seu consentimento".

(131) Dice: *"Vender ou expor à venda fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente: Pena – reclusão, de 4 (quatro) a 8 (oito) anos, e multa".*

(132) Con esta redacción: *"Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente: Pena – reclusão, de 3 (três) a 6 (seis) anos, e multa.*
§ 1 Nas mesmas penas incorre quem:
I – assegura os meios ou serviços para o armazenamento das fotografias, cenas ou imagens de que trata o caput deste artigo;
II – assegura, por qualquer meio, o acesso por rede de computadores às fotografias, cenas ou imagens de que trata o caput deste artigo.
§ 2 As condutas tipificadas nos incisos I e II do § 1 deste artigo são puníveis quando o responsável legal pela prestação do serviço, oficialmente notificado, deixa de desabilitar o acesso ao conteúdo ilícito de que trata o caput deste artigo".

el 241-B,[133] referido a la punición de la simple tenencia de material pornográfico infantil; el 241-C;[134] que incorpora la punición de las escenas simuladas, también incluidas en la previsión de aclaración conceptual en el art. 241-E;[135] y, finalmente, el art. 241-D[136], referido la punición del *grooming*.

b.3 **Chile**: en la ley 19.927 —14 de enero de 2004—, que modifica tanto al código sustantivo como al adjetivo, se trata la pornografía infantil; entre otros delitos contra la integridad sexual de los menores. En lo que hace al código sustantivo, que es el que aquí interesa, los tipos de relevancia son:

(133) Su texto: "*Adquirir, possuir ou armazenar, por qualquer meio, fotografia, vídeo ou outra forma de registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:*
Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa.
§ 1 A pena é diminuída de 1 (um) a 2/3 (dois terços) se de pequena quantidade o material a que se refere o caput deste artigo.
§ 2 Não há crime se a posse ou o armazenamento tem a finalidade de comunicar às autoridades competentes a ocorrência das condutas descritas nos arts. 240, 241, 241-A e 241-C desta Lei, quando a comunicação for feita por:
I – agente público no exercício de suas funções;
II – membro de entidade, legalmente constituída, que inclua, entre suas finalidades institucionais, o recebimento, o processamento e o encaminhamento de notícia dos crimes referidos neste parágrafo;
III – representante legal e funcionários responsáveis de provedor de acesso ou serviço prestado por meio de rede de computadores, até o recebimento do material relativo à notícia feita à autoridade policial, ao Ministério Público ou ao Poder Judiciário.
§ 3 As pessoas referidas no § 2 deste artigo deverão manter sob sigilo o material ilícito referido".

(134) Dice: "*Simular a participação de criança ou adolescente em cena de sexo explícito ou pornográfica por meio de adulteração, montagem ou modificação de fotografia, vídeo ou qualquer outra forma de representação visual: Pena – reclusão, de 1 (um) a 3 (três) anos, e multa.*
Parágrafo único. Incorre nas mesmas penas quem vende, expõe à venda, disponibiliza, distribui, publica ou divulga por qualquer meio, adquire, possui ou armazena o material produzido na forma do caput deste artigo".

(135) Con la siguiente redacción: "*Para efeito dos crimes previstos nesta Lei, a expressão "cena de sexo explícito ou pornográfica" compreende qualquer situação que envolva criança ou adolescente em atividades sexuais explícitas, reais ou simuladas, ou exibição dos órgãos genitais de uma criança ou adolescente para fins primordialmente sexuais*".

(136) Su texto: "*Aliciar, assediar, instigar ou constranger, por qualquer meio de comunicação, criança, com o fim de com ela praticar ato libidinoso: Pena – reclusão, de 1 (um) a 3 (três) anos, e multa.*
Parágrafo único. Nas mesmas penas incorre quem:
I – facilita ou induz o acesso à criança de material contendo cena de sexo explícito ou pornográfica com o fim de com ela praticar ato libidinoso;
II – pratica as condutas descritas no caput deste artigo com o fim de induzir criança a se exibir de forma pornográfica ou sexualmente explícita".

los arts. 366 *quáter,*[137] referido a conductas de significación sexual frente a menores; 366 *quinquies,*[138] referido a producción de material pornográfico con menores; 374 *bis,* [139] referido a cadena de comercialización a exhibición en cualquier soporte del material prohibido, así como adquisición y almacenamiento de aquél; y 374 *ter*,[140] que fija competencia a partir de un punto de acceso en territorio chileno.

b.4 **Colombia**: los tipos penales concernientes a la pornografía infantil han quedado delineados mediante sendas reformas al C.P. del año 2009: la pornografía con personas menores de 18 años (ley 1336, art. 218)[141] y la utilización o fa-

(137) Su texto: "Artículo 366 *quáter.* El que, sin realizar una acción sexual en los términos anteriores, para procurar su excitación sexual o la excitación sexual de otro, realizare acciones de significación sexual ante una persona menor de catorce años, la hiciere ver o escuchar material pornográfico o presenciar espectáculos del mismo carácter, será castigado con presidio menor en su grado medio a máximo.
Si, para el mismo fin de procurar su excitación sexual o la excitación sexual de otro, determinare a una persona menor de catorce años a realizar acciones de significación sexual delante suyo o de otro, la pena será presidio menor en su grado máximo.
Con iguales penas se sancionará a quien realice alguna de las conductas descritas en los incisos anteriores con una persona menor de edad pero mayor de catorce años, concurriendo cualquiera de las circunstancias del numerando 1° del art. 361 o de las enumeradas en el art. 363".

(138) Dice: "Artículo 366 *quinquies.* El que participare en la producción de material pornográfico, cualquiera sea su soporte, en cuya elaboración hubieren sido utilizados menores de dieciocho años, será sancionado con presidio menor en su grado máximo.
Para los efectos de este artículo y del art. 374 *bis,* se entenderá por material pornográfico en cuya elaboración hubieren sido utilizados menores de dieciocho años, toda representación de éstos dedicados a actividades sexuales explícitas, reales o simuladas, o toda representación de sus partes genitales con fines primordialmente sexuales".

(139) Tiene la siguiente redacción: "Artículo 374 *bis.* El que comercialice, importe, exporte, distribuya, difunda o exhiba material pornográfico, cualquiera sea su soporte, en cuya elaboración hayan sido utilizados menores de dieciocho años, será sancionado con la pena de presidio menor en su grado medio a máximo.
El que maliciosamente adquiera o almacene material pornográfico, cualquiera sea su soporte, en cuya elaboración hayan sido utilizados menores de dieciocho años, será castigado con presidio menor en su grado medio".

(140) Su texto: "Artículo 374 *ter.* Las conductas de comercialización, distribución y exhibición señaladas en el artículo anterior, se entenderán cometidas en Chile cuando se realicen a través de un sistema de telecomunicaciones al que se tenga acceso desde territorio nacional".

(141) Su texto: "El que fotografíe, filme, grabe, produzca, divulgue, ofrezca, venda, compre, posea, porte, almacene, trasmita o exhiba, por cualquier medio, para uso personal o intercambio, representaciones reales de actividad sexual que involucre persona menor de 18 años de edad, incurrirá en prisión de 10 a 20 años y multa de 150 a 1500 salarios mínimos legales mensuales vigentes.
Igual pena se aplicará a quien alimente con pornografía infantil bases de datos de Internet, con o sin fines de lucro.
La pena se aumentará de una tercera parte a la mitad cuando el responsable sea integrante de la familia de la víctima".

cilitación de medios de comunicación para ofrecer actividades sexuales con personas menores de 18 años (ley 1329, art. 219-A).[142]

b.5 **Ecuador**: mediante la ley 2005-2 —23 de junio de 2005— introdujo en su CP un capítulo sin número concerniente a los "Delitos de Explotación Sexual" que, a través de varios artículos también sin número, pune la pornografía infantil entre otras conductas disvaliosas que incluyen hasta la oferta de turismo sexual. La norma que aquí interesa es el primer artículo sin número.[143]

b.6 **Paraguay**: la ley 2861/06 —"De represión del comercio y la difusión comercial o no comercial de material pornográfico, utilizando la imagen u otra representación de menores o incapaces"— introdujo la punición de la utilización de niños, niñas y adolescentes en pornografía (art. 1°) o su exhibición en actos sexuales (art. 3°); la difusión o comercialización de pornografía infantil (art. 2°), contemplándose diversas situaciones agravantes (art. 4°). Luego, la reforma del CP por ley 4439 —año 2011— modificó el art. 140[144], que es el ahora regente. Entre su variado catálogo

(142) Dice: "El que utilice o facilite el correo tradicional, las redes globales de información, telefonía o cualquier medio de comunicación, para obtener, solicitar, ofrecer o facilitar contacto o actividad con fines sexuales con personas menores de 18 años de edad, incurrirá en pena de prisión de diez (10) a catorce (14) años y multa de sesenta y siete (67) a (750) salarios mínimos legales mensuales vigentes.
Las penas señaladas en el inciso anterior se aumentarán hasta en la mitad ($^1/_2$) cuando las conductas se realizaren con menores de catorce (14) años".

(143) En su parte pertinente dice: "art. … (1). (Agregado por el art. 18 de la ley 2005-2, R.O. 45, 23-VI-2005). Quien produjere, publicare o comercializare imágenes pornográficas, materiales visuales, audiovisuales, informáticos, electrónicos o de cualquier otro soporte físico o formato, u organizare espectáculos en vivo, con escenas pornográficas en que participen los mayores de catorce y menores de dieciocho años, será reprimido con la pena de seis a nueve años de reclusión menor ordinaria, el comiso de los objetos y de los bienes producto del delito, la inhabilidad para el empleo, profesión u oficio.

Con la misma pena incurrirá quien distribuyere imágenes pornográficas, cuyas características externas hiciere manifiesto que en ellas sea (SIC) grabado o fotografiado la exhibición de mayores de doce y menores de dieciocho años al momento de creación de la imagen.

Con la misma pena será reprimido quien facilitare el acceso a espectáculos pornográficos o suministrare material pornográfico en cuyas imágenes participen menores de edad…".

(144) Dice: "Pornografía relativa a niños y adolescentes.

1° El que:

1) produjere publicaciones, en el sentido del art. 14, inc. 3, que representen actos sexuales con participación de personas menores de dieciocho años de edad o la exhibición de sus partes genitales;
2) organizara, financiara o promocionara espectáculos, públicos o privados, en los que participe una persona menor de dieciocho años en la realización de actos sexuales, o;
3) distribuyera, importara, exportara, ofertara, canjeara, exhibiera, difundiera, promocionara o financiara la producción o reproducción de publicaciones en sentido del numeral 1, será castigado con pena privativa de libertad de hasta cinco años o multa.

de conductas típicas, incluye la simple posesión de material prohibido (parág. 4°).

b.7 **Perú**: por la modificación al art. 181-A[145] del CP mediante ley 29.408 —del 18 de septiembre de 2009— se tipificó la promoción, publicidad, favorecimiento o facilitación de la explotación sexual comercial de menores por cualquier medio; incluyendo expresamente los electrónicos, magnéticos y a través de Internet. A su vez, dentro de las ofensas al pudor público, el artículo 182-A sanciona la publicación en los medios de comunicación sobre delitos de libertad sexual a menores. Más específicamente a nuestro objeto, el art. 183 pena las exhibiciones y publicaciones obscenas de menores; y el artículo 183-A[146] —modificado por ley 28.251 del 8 de junio

2° El que reprodujera publicaciones según el numera l 1 del inc. 1, será castigado con pena privativa de libertad de hasta tres años o multa.

3° La pena de los incisos anteriores podrá ser aumentada hasta diez años cuando:

1) las publicaciones y espectáculos en el sentido de los incs. 1 y 2 se refieran a menores de catorce años o se dé acceso a los menores de dicha edad a publicaciones y espectáculos, en sentido de los incisos citados;
2) el autor tuviera la patria potestad, deber de guarda o tutela del niño o adolescente, o se le hubiere confiado la educación o cuidado del mismo;
3) el autor operara en connivencia con personas a quienes competa un deber de educación, guarda o tutela respecto del niño o adolescente;
4) el autor hubiere procedido, respecto del niño o adolescente, con violencia, fuerza, amenaza, coacción, engaño, recompensa o promesa remuneratoria de cualquier especie; o
5) el autor actuara comercialmente o como miembro de una banda dedicada a la realización reiterada de los hechos punibles señalados.

4° El que obtuviera la posesión de publicaciones en el sentido de los incs. 1 y 3, será castigado con pena privativa de libertad d e hasta tres años o con multa.

5° Se aplicará, en lo pertinente, también lo dispuesto en los arts. 57 y 94".

(145) Dice: "Artículo 181-A. Explotación sexual comercial infantil y adolescente en ámbito del turismo
El que promueve, publicita, favorece o facilita la explotación sexual comercial en el ámbito del turismo, a través de cualquier medio escrito, folleto, impreso, visual, audible, electrónico, magnético o a través de Internet, con el objeto de ofrecer relaciones sexuales de carácter comercial de personas de catorce (14) y menos de dieciocho (18) años de edad será reprimido con pena privativa de libertad no menor de cuatro (4) ni mayor de ocho (8) años.
Si la víctima es menor de catorce años, el agente, será reprimido con pena privativa de la libertad no menor de seis (6) ni mayor de ocho (8) años.
El agente también será sancionado con inhabilitación conforme al art. 36 incs. 1, 2, 4 y 5.
Será no menor de ocho (8) ni mayor de diez (10) años de pena privativa de la libertad cuando ha sido cometido por autoridad pública, sus ascendientes, maestro o persona que ha tenido a su cuidado por cualquier título a la víctima".

(146) En su parte pertinente dice: "Artículo 183-A. Pornografía infantil. El que posee, promueve, fabrica, distribuye, exhibe, ofrece, comercializa o publica, importa o exporta por cualquier medio objetos, libros, escritos, imágenes, videos o audios, o realiza espectáculos en vivo de carácter pornográfico, en los cuales se utilice a personas de catorce y menos de

de 2004— se ocupa de la pornografía infantil. La disposición complementaria modificatoria cuarta de este último ha sido modificada por vía de la ley 30.096 —año 2013—. El cambio más significativo es la referencia a su comisión por cualquier medio y un incremento significativo de la escala de pena conminada en abstracto.

Además, la citada nueva Ley de Delitos Informáticos ha incorporado el tipo de "Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos"(art. 5)[147] en el marco del capítulo III, "Delitos Informáticos contra la indemnidad y libertad sexuales". Se trata de la conducta conocida como *grooming*.

Finalmente, en la primera de sus disposiciones complementarias finales, "Codificación de la pornografía infantil"; aclara que la Policía Nacional del Perú puede mantener tal mantener en sus archivos, con autorización y supervisión del Ministerio Público, tal material para fines exclusivos del cumplimiento de su función en una base de datos debidamente codificada.

b.8 **Uruguay**: el viejo artículo 278[148] del CP mantiene la punición de la pornografía en general. No obstante, por ley 17.559 —del 27 de septiembre de 2002— se aprobó 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 pornografía. Además, por ley 17.815 —del 6 de noviembre de 2004—, se reguló la "Violencia sexual comercial o no co-

dieciocho años de edad, será sancionado con pena privativa de libertad no menor de seis ni mayor de diez años y con ciento veinte a trescientos sesenta y cinco días multa.

La pena privativa de libertad será no menor de diez ni mayor de doce años y de cincuenta a trescientos sesenta y cinco días multa cuando:

1. El menor tenga menos de catorce años de edad.
2. El material pornográfico se difunda a través de las tecnologías de la información o de la comunicación.

Si la víctima se encuentra en alguna de las condiciones previstas en el último párrafo del art. 173 o si el agente actúa en calidad de integrante de una organización dedicada a la pornografía infantil, la pena privativa de libertad será no menor de doce ni mayor de quince años. De ser el caso, el agente será inhabilitado conforme los numerales 1, 2 y 4 del art. 36".

(147) Su texto: El que, a través de las tecnologías de la información o de la comunicación, contacta con un menor de catorce años para solicitar u obtener de él material pornográfico, o para llevar a cabo actividades sexuales con él, será reprimido con pena privativa de libertad no menor de cuatro ni mayor de ocho años e inhabilitación conforme a los numerales 1, 2 y 4 del art. 36 del CP.

Cuando la víctima tiene entre catorce y menos de dieciocho años de edad y medie engaño, la pena será no menor de tres ni mayor de seis años e inhabilitación conforme a los numerales 1, 2 y 4 del art. 36 del CP".

(148) Dice: "Comete delito de exhibición pornográfica el que ofrece públicamente espectáculos teatrales o cinematográficos obscenos, el que transmite audiciones o efectúa publicaciones de idéntico carácter. Este delito se castiga con la pena de tres a veinticuatro meses de prisión".

mercial cometida contra niños, adolescentes e incapaces". Así se consagraron varios nuevos tipos penales: la fabricación o producción de material pornográfico con utilización de personas menores de edad o incapaces (art. 1°);[149] el comercio y difusión de material pornográfico en que aparezca la imagen u otra forma de representación de personas menores de edad o personas incapaces (art. 2°);[150] favorecer la comercialización y difusión de material pornográfico con la imagen u otra representación de una o más personas menores de edad o incapaces (art. 3°);[151] la retribución o promesa de retribución a personas menores de edad o incapaces para que ejecuten actos sexuales o eróticos de cualquier tipo (art. 4°);[152] la contribución a la explotación sexual de personas menores de edad o incapaces (art. 5°) [153] y el tráfico de personas menores de edad o incapaces (art. 6°).[154]

b.9 **Venezuela**: en el capítulo IV "De los delitos contra niños, niñas o adolescentes" de la LECDI de 2001 se pune la difusión o exhibición de material por-

(149) Con la siguiente redacción: "El que de cualquier forma fabricare o produjere material pornográfico utilizando a personas menores de edad o personas mayores de edad incapaces, o utilizare su imagen, será castigado con pena de veinticuatro meses de prisión a seis años de penitenciaría".

(150) Su texto: "El que comerciare, difundiere, exhibiere, almacenare con fines de distribución, importare, exportare, distribuyere u ofertare material pornográfico en el que aparezca la imagen o cualquier otra forma de representación de una persona menor de edad o persona incapaz, será castigado con pena de doce meses de prisión a cuatro años de penitenciaría".

(151) Su texto: "El que de cualquier modo facilitare, en beneficio propio o ajeno, la comercialización, difusión, exhibición, importación, exportación, distribución, oferta, almacenamiento o adquisición de material pornográfico que contenga la imagen o cualquier otra forma de representación de una o más personas menores de edad o incapaces será castigado con pena de seis meses de prisión a dos años de penitenciaría. A los efectos del presente artículo y de los anteriores, se entiende que es producto o material pornográfico todo aquel que por cualquier medio contenga la imagen u otra forma de representación de personas menores de edad o incapaces dedicadas a actividades sexuales explícitas, reales o simuladas, o la imagen o representación de sus partes genitales, con fines primordialmente sexuales".

(152) Dice: "El que pagare o prometiere pagar o dar a cambio una ventaja económica o de otra naturaleza a persona menor de edad o incapaz de cualquier sexo, para que ejecute actos sexuales o eróticos de cualquier tipo, será castigado con pena de dos a doce años de penitenciaría".

(153) Su redacción es: "El que de cualquier modo contribuyere a la prostitución, explotación o servidumbre sexual de personas menores de edad o incapaces, será castigado con pena de dos a doce años de penitenciaría. La pena será elevada de un tercio a la mitad si se produjere con abuso de las relaciones domésticas o de la autoridad o jerarquía, pública o privada, o la condición de funcionario policial del agente".

(154) Su texto: "El que de cualquier modo favorezca o facilite la entrada o salida del país de personas menores de edad o incapaces, para ser prostituidas o explotadas sexualmente, será castigado con pena de dos a doce años de penitenciaría".

nográfico (art. 23)[155] y la exhibición pornográfica de niños o adolescentes (art. 24)[156] usando tecnologías de información.

c. **Bolivia** no ha actualizado su legislación. Pese a tener un código relativamente joven, de 1997, mantuvo la tradicional punición de los llamados "ultrajes al pudor" en sus artículos 323[157] y 324.[158]

5 | Infracciones vinculadas a los atentados a la propiedad intelectual y derechos afines

5.1 | Afectación de la propiedad intelectual y derechos afines (art. 10)

Al igual que en el caso anterior, el Título 4 de la Sección 1 —"Infracciones vinculadas a los atentados a la propiedad intelectual y a los derechos afines"— está integrado por el artículo referido a la "Afectación de la propiedad intelectual y derechos afines" (art. 10), con el siguiente texto:

> 1. "Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, los atentados a la propiedad

(155) Dice: "Todo aquel que, por cualquier medio que involucre el uso de tecnologías de información, exhiba, difunda, transmita o venda material pornográfico o reservado a personas adultas, sin realizar previamente las debidas advertencias para que el usuario restrinja el acceso a niños, niñas y adolescentes, será sancionado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias".

(156) Con esta redacción: "Toda persona que por cualquier medio que involucre el uso de tecnologías de la información, utilice a la persona o imagen de un niño, niña o adolescente con fines exhibicionistas o pornográficos, será penada con prisión de cuatro a ocho años y multa de cuatrocientas a ochocientas unidades tributarias".

(157) Dice: "(Actos Obscenos). El que en lugar público o expuesto al público realizare actos obscenos o los hiciere ejecutar por otro, incurrirá en reclusión de tres meses a dos años".

(158) Su texto: "(Publicaciones y Espectáculos Obscenos). El que con cualquier propósito expusiere públicamente, fabricare, introdujere en el país o reprodujere libros, escritos, dibujos, imágenes u otros objetos obscenos, o el que los distribuyere o pusiere en circulación, o el que públicamente ofreciere espectáculos teatrales o cinematográficos u otros obscenos, o transmitiere audiciones de la misma índole, será sancionado con reclusión de tres meses a dos años".

intelectual definida por la legislación de cada Estado, conforme a las obligaciones que haya asumido por aplicación de la Convención Universal sobre los Derechos de Autor, revisada en París el 24 de julio de 1971, del Convenio de Berna para la protección de obras literarias y artísticas, del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del Tratado de la OMPI sobre Derecho de Autor, a excepción de cualquier derecho moral conferido por dichas Convenciones, cuando tales actos sean cometidos deliberadamente, a escala comercial y a través de un sistema informático.

2. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, los atentados a los derechos afines definidos por la legislación de cada Estado, conforme a las obligaciones que haya asumido por aplicación de la Convención Internacional sobre la Protección de los Artistas Intérpretes o Ejecutantes, los Productores de Fonogramas y los Organismos de Radiodifusión, hecha en Roma (Convención de Roma), del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del Tratado de la OMPI sobre interpretación o ejecución y fonogramas, a excepción de cualquier derecho moral conferido por dichas Convenciones, cuando tales actos sean cometidos deliberadamente, a escala comercial y a través de un sistema informático.

3. Las Partes podrán, de concurrir determinadas circunstancias, reservarse el derecho de no imponer responsabilidad penal en aplicación de los párrs. 1 y 2 del presente artículo, siempre que se disponga de otros recursos eficaces para su represión y que dicha reserva no comporte infracción de las obligaciones internacionales que incumban al Estado por aplicación de los instrumentos internacionales mencionados en los párrs. 1 y 2 del presente artículo".

a. En materia de atentados contra la propiedad intelectual o derechos afines; no debe perderse de vista que el Convenio habla de una posible intervención penal, cuando se trate de conductas dolosas a través de un

sistema informático y tengan "escala comercial". Podría prescindirse de ésta si se dispusiera de otros recursos eficaces para su represión.

b. En este caso, puede afirmarse que todos los países que integran la región poseen legislación que cubre la materia.

b.1 **Argentina**: la ley 25.036 —año 1998— modificó la Ley de Propiedad Intelectual (LPI), ley 11.723, para brindar protección penal al *software* a partir de la inclusión de los programas de computación (arts. 1°, 4°, 9°, 55 *bis* y 57). Así se ampliaron los objetos de protección de las conductas que ya se tipificaban en los arts. 71, (159) 72 y ss., que permanecieron inalterados.

Por ley 26.285 —BO 13/09/07—, se introdujo otra modificación a la LPI que recorta el universo de supuestos típicos en términos de lesividad en el aspecto patrimonial, eximiendo del pago de derechos de autor a la reproducción y distribución de obras científicas o literarias en sistemas especiales para ciegos y personas con otras discapacidades perceptivas; siempre que la reproducción y distribución sean hechas por entidades autorizadas. Ésto rige también para las obras que se distribuyan por vía electrónica, encriptadas o protegidas por cualquier otro sistema que impida su lectura a personas no habilitadas. El acceso a a las obras protegidas está a cargo de aquellas entidades autorizadas a asignar y administrar las claves de acceso. Conforme el artículo 36,(160) no se aplicará la exención a la reproducción y distribución de obras que se hubieron editado originalmente en sistemas especiales para personas con discapacidades visuales o perceptivas y que se hallen comercialmente disponibles.

Además del *software* como objeto de la llamada "piratería", hay otras variadas expresiones de propiedad intelectual afectadas. El vocablo se aplica de forma genérica —y despectiva— a todas aquellas personas que descargan archivos con el más diverso material audiovisual desde Internet en forma gratuita y presuntamente violando los derechos emergentes de aquélla. En el caso de la música y las películas y programas seriales de televisión, la cantidad de descargas es prácticamente incalculable. La

(159) Limito la transcripción a este tipo porque es el básico y dice: "Será reprimido con la pena establecida por el art. 172 del Código Penal el que de cualquier manera y en cualquier forma defraude los derechos de propiedad intelectual que reconoce esta ley". La escala penal conminada en abstracto, por integración, es de un mes a seis años de prisión.

(160) Quedó con la siguiente redacción: "Asimismo, advertirán (las obras reproducidas y distribuidas en sistemas especiales) que el uso indebido de estas reproducciones será reprimido con pena de prisión, conforme el art. 172 del Código Penal".

masividad en el uso de los archivos MP3 y MP4, así como de las redes P2P, constituye en verdadero fenómeno social y cultural que lleva a preguntarse si tiene sentido la persecución penal de una conducta socialmente aceptada —¿teoría de la adecuación social?—. Así, Carnevale plantea la necesidad de analizar si realmente estamos frente a un problema social o es una lucha de intereses económicos lo que, sencillamente, está en juego.(161)

Otra norma relacionada de interés es la ley 24.766 —año 1997— de "Confidencialidad sobre información y productos que estén legítimamente bajo control de una persona y se divulgue indebidamente de manera contraria a los usos comerciales honestos". Ésta introdujo la protección del secreto de las informaciones de personas físicas o jurídicas almacenadas en medios informáticos —bases de datos—, penándose su ilegítima divulgación con una multa de $ 1500 a $ 90.000 e inhabilitación especial de seis meses a tres años (art. 156); conforme lo establecido por el CP para el delito de violación de secretos. Concretó así la protección de la información secreta, confidencial, de la empresa y personas físicas; conforme al artículo 39 del Acuerdo sobre los Derechos de la Propiedad Intelectual suscripto por nuestro país y aprobado por ley 24.425.

b.2 **Bolivia**: la protección penal del *software* ha sido recogida a partir del artículo 6° de la ley 1322 de Derechos de Autor, cuyo inc. l indica: "Los programas de ordenador o computación (soporte lógico o *software*), bajo reglamentación específica", como obras amparadas por la ley. El artículo 65 indica, con relación a las violaciones al derecho autoral y sus sanciones penales, que los procesos serán de conocimiento de la judicatura penal ordinaria y que las sanciones serán las previstas por el artículo 362(162) del CP.

b.3 **Brasil**: además del artículo 184 del CP, por la ley 7646 —del 18 de diciembre de 1987— se consideró al *software* un derecho autoral y se consagró un tipo delictivo específico: **Violar derechos de autor de programas de ordenador**; con una pena que puede ser de 6 (seis) meses de detención a 2 (dos) años y multa (art. 35):

(161) Carnevale, Carlos A., "¿Es posible ser condenado penalmente por descargar música de Internet? – Mp3, P2P y garantías constitucionales", en *el Suplemento de Derecho de la Alta Tecnología de la Biblioteca Jurídica Online* ", [en línea] www.elDial.com.ar, 12/3/08.

(162) Dice: "El que de manera arbitraria y por cualquier medio explotare o dispusiere, publicare o reprodujere una obra literaria, científica o artística, en perjuicio de los derechos de su legítimo autor, siempre que éste hubiera reservado sus derechos o los hubiere inscrito en los registros respectivos, será sancionado con reclusión de tres meses a dos años y multa de treinta a sesenta días".

Con posterioridad, siguiendo con el marco de protección dentro del derecho autoral, se dictó la Ley de Software 9609/98, reglamentada por Decreto 255/98, en la que se tipificó el delito de copia no autorizada de *software*. Su artículo 12[163] comprende, en opinión de Vianna, tres figuras distintas que, en la jerga informática, se conocen como piratería, *warez* y *crakz*, aún cuando no marca expresamente las diferencias e impresiona haber sido creado atendiendo sólo a la primera.[164] Llama la atención que, para la primera, no se incluye como exigencia típica el ánimo de lucro. Más, el parág. 1° prevé pena agravada cuando la conducta se realiza para beneficio económico. El *warez*[165] se diferencia por la carencia del pasaje del programa a un medio físico similar. La práctica consiste en poner a disposición en Internet, en algún servidor gratuito, el programa para que puedan ser "bajados" o copiados por cualquiera que acceda al sitio. Esta facilitación generalmente no persigue ningún beneficio económico sino que el ilícito se realiza presidido por una concepción ideológica que atribuye a las empresas de *software* un excesivo ánimo de lucro por el que abusan de sus derechos autorales cobrando precios excesivos. Los *crackz* son pequeños programas que permiten quebrar los códigos de seguridad que limitan el uso de programas de demostración (demos) o de experimentación previa a la compra *(sharewares)*, con lo que los tornan completos sin el pago de los derechos autorales.

b.4 **Chile**: la piratería del *software* se encuentra regida por la ley 17.336 de Derechos de Autor —año 1970—, varias veces modificada, a la que se incorporaran conceptos como "programa computacional" (art. 3° inc. 16)

(163) Dice: *"art. 12. Violar direitos de autor de programa de computador: Pena – Detenção de seis meses a dois anos ou multa. § 1° Se a violação consistir na reprodução, por qualquer meio, de programa de computador, no todo ou em parte, para fins de comércio, sem autorização expressa do autor ou de quem o represente: Pena – Reclusão de um a quatro anos e multa. § 2° Na mesma pena do parágrafo anterior incurre quem vende, expõe à venda, introduz no País, adquire, oculta ou tem em depósito, para fins de comércio, original ou cópia de programa de computador, producido com violação de direito autoral. § 3° Nos crimes previstos neste artigo, somente se procede mediante queixa, salvo: I- quando praticados em prejuízo de entidade de direito público, autarquía, empresa pública, sociedade de encomia mista ou fundação instituída pelo poder público; II- quando, em decorrência de ato delituoso, resultar sonegação fiscal, perda de arrecadação tributária ou prática de quaisquer dos crimes contra a ordem tributária ou contra as relações de consumo. § 4° No caso de inciso II do parágrafo anterior, a exigibilidade do tributo, ou contribuição social e qualquer accesorio, procesar-se-á independentemente de representação.*

(164) Lima Vianna, Túlio, "Dos crimes por computador", en *el portal jurídico "Mundo Jurídico"* [en línea] www.mundojuridico.adv.br, en 16/4/03, parág. 3.

(165) El término proviene de la palabra inglesa "*wares*": mercadería. El cambio de la "s" por la "z", se debe a que en la terminología informal informática el sufijo "z" sirve para identificar todo aquello que es ilegal (ver Vianna, *op. cit.*, parág. 3.2).

y "copia de programa computacional" (art. 5° inc. t). Los tipos penales son los arts. 79,[166] 80[167] y 81.[168]

b.5. **Colombia**: la "violación de los derechos morales de autor" se encuentra prevista en el artículo 270 del CP,[169] reformado por ley 890 del 10 de enero de

.....

(166) Dice: "art. 79. Cometen delito contra la propiedad intelectual y serán sancionados con la pena de presidio menor en su grado mínimo y multa de 5 a 50 unidades tributarias mensuales:

a) Los que, sin estar expresamente facultados para ello, utilicen obras de dominio ajeno protegidas por esta ley, inéditas o publicadas, en cualquiera de las formas o por cualquiera de los medios establecidos en el art. 18;

b) Los que, sin estar expresamente facultados para ello, utilicen las interpretaciones, producciones y emisiones protegidas de los titulares de los derechos conexos, con cualquiera de los fines o por cualquiera de los medios establecidos en el Título II de esta ley.

c) Los que falsifiquen obras protegidas por esta ley, sean literarias, artísticas o científicas, o las editen, reproduzcan o vendan ostentando falsamente el nombre del editor autorizado, suprimiendo o cambiando el nombre del autor o el título de la obra, o alterando maliciosamente su texto;

d) Los que, obligados al pago de retribución por derecho de autor o conexos derivados de la ejecución de obras musicales, omitieren la confección de las planillas de ejecución correspondiente, y

e) Los que falsificaren o adulteraren una planilla de ejecución".

(167) Su texto: "art. 80. Cometen, asimismo, delito contra la propiedad intelectual y serán sancionados con las penas que se indican en cada caso:

a) Los que falsearen el número de ejemplares vendidos efectivamente, en las rendiciones de cuentas a que se refiere el art. 50, serán sancionados con las penas establecidas en el art. 467 del CP, y

b) Los que, en contravención a las disposiciones de esta ley o a los derechos que ella protege, intervengan, con ánimo de lucro, en la reproducción, distribución al público o introducción al país, y los que adquieran o tengan con fines de venta: fonogramas, videogramas, discos fonográficos, cassettes, videocasetes, filmes o películas cinematográficas o programas computacionales.

Los autores serán sancionados con la pena de presidio o reclusión en su grado mínimo, aumentándose en un grado en caso de reincidencia".

(168) Dice: "art. 81. El que a sabiendas publicare o exhibiere una obra perteneciente al patrimonio cultural común bajo un nombre que no sea el del verdadero autor, será penado con una multa de dos a cuatro sueldos vitales anuales, escala A), del departamento de Santiago.
El recurrente puede pedir, además, la prohibición de la venta, circulación o exhibición de los ejemplares".

(169) Su texto: "Incurrirá en prisión de treinta y dos (32) a noventa (90) meses y multa de veinte seis punto sesenta y seis (26.66) a trescientos (300) salarios mínimos legales mensuales vigentes quien:

1. Publique, total o parcialmente, sin autorización previa y expresa del titular del derecho, una obra inédita de carácter literario, artístico, científico, cinematográfico, audiovisual o fonograma, programa de ordenador o soporte lógico.

2004, incluyendo expresas a menciones programas de ordenador y soportes lógicos.

b.6 **Ecuador**: en su Ley de Propiedad Intelectual, ley 83 —año 1998—, los programas de ordenador se consideran "objeto de derechos de autor" (art. 8 inc. k) y gozan de idéntica protección que las obras literarias y demás elementos allí descriptos, lo que se complementa en el art. 28.[170] Los tipos penales, con profusa variedad de conductas alternativas consideradas, se encuentran en los artículos 319 a 325. El artículo 327 introduce circunstancias agravantes especiales. El primero, tipo básico que abre el capítulo, prevé una pena de 3 meses a 3 años de prisión y multa de 500 a 5000 unidades de valor constante (UVC).

b.7 **Paraguay**: rige el artículo 184[171] del CP —año 1998—, en función de la ley 1328/1998 "De Derecho de Autor y Derechos Conexos".

2. Inscriba en el registro de autor con nombre de persona distinta del autor verdadero, o con título cambiado o suprimido, o con el texto alterado, deformado, modificado o mutilado, o mencionando falsamente el nombre del editor o productor de una obra de carácter literario, artístico, científico, audiovisual o fonograma, programa de ordenador o soporte lógico.
3. Por cualquier medio o procedimiento compendie, mutile o transforme, sin autorización previa o expresa de su titular, una obra de carácter literario, artístico, científico, audiovisual o fonograma, programa de ordenador o soporte lógico.

Parágrafo: Si en el soporte material, carátula o presentación de una obra de carácter literario, artístico, científico, fonograma, videograma, programa de ordenador o soporte lógico, u obra cinematográfica se emplea el nombre, razón social, logotipo o distintivo del titular legítimo del derecho, en los casos de cambio, supresión, alteración, modificación o mutilación del título o del texto de la obra, las penas anteriores se aumentarán hasta en la mitad".

(170) Dice: "Los programas de ordenador se consideran obras literarias y se protegen como tales. Dicha protección se otorga independientemente de que hayan sido incorporados en un ordenador y cualquiera sea la forma en que estén expresados, ya sea en forma legible por el hombre (código fuente) o en forma legible por máquina (código objeto), ya sean programas operativos y programas aplicativos, incluyendo diagramas de flujo, planos, manuales de uso, y en general, aquellos elementos que conformen la estructura, secuencia y organización del programa".

(171) Tiene la siguiente redacción: "Artículo 184. Violación del derecho de autor o inventor. 1° El que sin autorización del titular: 1) divulgara, promocionara, reprodujera o públicamente representara una obra de literatura, ciencia o arte, protegida por el derecho de autor; o 2) exhibiera públicamente el original o una copia de una obra de las artes plásticas o visuales, protegida por el derecho de autor, será castigado con pena privativa de libertad de hasta tres años o con multa. 2° A las obras señaladas en el inciso anterior se equipararán los arreglos y otras adaptaciones protegidas por el derecho de autor. 3° Con la misma pena será castigado el que falsificara, imitara o, sin autorización del titular: 1) promocionara una marca, un dibujo o un modelo industrial o un modelo de utilidad, protegidos; o 2) utilizara una invención protegida por patente. 4° La persecución penal del hecho dependerá de la instancia de la víctima. 5° En caso de condena a una pena se aplicará, a petición de la víctima o del ministerio público, lo dispuesto en el art. 60".

b.8 **Perú**: en su CP de 1991 se protegen los derechos intelectuales —Título VII—, distinguiendo los de autor y conexos —capítulo I— y la propiedad industrial —capítulo II—. El tipo genérico de fabricación o uso no autorizado de patente es protegido por el artículo 222; con versión actualizada, en la que se incluyen nuevas tecnologías.

En cuanto al capítulo I, la copia o reproducción no autorizada se prevé en el art. 216 con una redacción abierta "u otro medio". La falta de mención de aspectos vinculados a las TIC se mantiene en el resto del articulado, a excepción del art. 218,(172) inc. d, que tipifica el plagio y la comercialización; y el art. 220-A,(173) referido a la elusión de medidas tecnológicas efectivas; 220-B,(174) referido a los productos destinados a eludir medidas tecnológicas; 220-C,(175) referido a los servicios destinados a la elusión de medidas tecnológicas; 220-E,[176] referido a las etiquetas, carátulas

(172) La parte pertinente dice: "d. Se fabrique, ensamble, importe, exporte, modifique, venda, alquile, ofrezca para la venta o alquiler, o ponga de cualquier otra manera en circulación dispositivos, sistemas tangibles o intangibles, esquemas o equipos capaces de soslayar otro dispositivo destinado a impedir o restringir la realización de copias de obras, o a menoscabar la calidad de las copias realizadas, o capaces de permitir o fomentar la recepción de un programa codificado, radiodifundido o comunicado en otra forma al público, por aquellos que no están autorizados para ello".

(173) Dice: "El que, con fines de comercialización u otro tipo de ventaja económica, eluda sin autorización cualquier medida tecnológica efectiva que utilicen los productores de fonogramas, artistas, intérpretes o ejecutantes, así como los autores de cualquier obra protegida por derechos de propiedad intelectual, será reprimido con pena privativa de libertad no mayor de dos años y de diez a sesenta días multa".

(174) Dice: "El que, con fines de comercialización u otro tipo de ventaja económica, fabrique, importe, distribuya, ofrezca al público, proporcione o de cualquier manera comercialice dispositivos, productos o componentes destinados principalmente a eludir una medida tecnológica que utilicen los productores de fonogramas, artistas intérpretes o ejecutantes, así como los autores de cualquier obra protegida por derechos de propiedad intelectual, será reprimido con pena privativa de libertad no mayor de dos años y de diez a sesenta días-multa".

(175) Su texto: "El que, con fines de comercialización u otro tipo de ventaja económica, brinde u ofrezca servicios al público destinados principalmente a eludir una medida tecnológica efectiva que utilicen los productores de fonogramas, artistas intérpretes o ejecutantes, así como los autores de cualquier obra protegida por derechos de propiedad intelectual, será reprimido con pena privativa de libertad no mayor de dos años y de diez a sesenta días-multa".

(176) Con esta redacción: "El que fabrique, comercialice, distribuya o almacene con fines comerciales etiquetas o carátulas no auténticas adheridas o diseñadas para ser adheridas a un fonograma, copia de un programa de ordenador, documentación o empaque de un programa de ordenador o a la copia de una obra cinematográfica o cualquier otra obra audiovisual, será reprimido con pena privativa de libertad no menor de tres años ni mayor de seis años y de sesenta a ciento veinte días-multa".

y empaques; y 220-F,[177] referido a los manuales, licencias u otra documentación, o empaques no auténticos relacionados a programas de ordenador. Éstos fueron reformados por ley 29.263 el 2 de octubre de 2008.

b.9 **Uruguay**: el 13 de enero de 2003 se promulgó la Ley de Protección del Derecho de Autor y Derechos Conexos, ley 17.616, que modifica el texto de la ley 9739 —año1937—. Se incluyó, así, al *software* como una de las obras objeto de su protección, regulando de esta forma su reproducción ilícita. También modificó los delitos relativos a violaciones a los derechos de autor. De tal suerte, el artículo 46 de la ley 9739[178] establece que: quien edite, venda, reproduzca o hiciere reproducir por cualquier medio o instrumento —total o parcialmente—, distribuya, almacene para distribuir al público o ponga a disposición del mismo en cualquier forma o medio con ánimo de lucro o de causar un perjuicio injustificado, una obra programa de ordenador inédita o publicada sin la autorización escrita de su respectiva titular, contraviniendo en cualquier forma lo dispuesto en la ley; será castigado con pena de tres meses de prisión a tres años de penitenciaría.

Por otra parte, quien reproduzca o hiciere reproducir por cualquier medio o procedimiento, sin ánimo de lucro o de causar un perjuicio injustificado un programa de ordenador sin la autorización escrita de su respectivo titular, será castigado con multa de 10 UR a 1500 UR. Se han agregado por la ley 17.616 otras figuras delictivas referidas a medidas tecnológicas e información sobre la gestión de derechos. Serán sancionados con pena de tres meses de prisión a tres años de penitenciaría en primer lugar, quien fabrique, importe, venda, dé en arrendamiento o ponga de cualquier otra manera en circulación dispositivos o productos, sus componentes o herramientas. En segundo lugar, quien preste cualquier servicio cuyo propósito sea impedir, burlar, eliminar, desactivar o eludir de cualquier forma los dispositivos técnicos que los titulares hayan dispuesto para proteger sus respectivos derechos. En tercer lugar, quien altere o suprima, sin autorización del titular de los derechos protegidos por dicha ley, la información electrónica colocada por los titulares de los derechos de autor o conexos, para posibilitar la gestión de sus derechos patrimoniales y morales; de modo que puedan perjudicarse estos derechos. Con idéntica sanción, en cuarto lugar, pune a quien distribuya, importe con fines de distribución, emita o comunique al público, sin autorización, ejemplares de obras, interpretaciones o fonogramas; sabiendo que la información electrónica colocada por

(177) Su texto: "El que elabore, comercialice, distribuya, almacene, transporte, transfiera o de otra manera disponga con fines comerciales u otro tipo de ventaja económica manuales, licencias u otro tipo de documentación, o empaques no auténticos para un programa de ordenador, será reprimido con pena privativa de libertad no menor de cuatro años ni mayor de seis años y de sesenta a ciento veinte días multa".

(178) Ver art. 15, ley 17.616

los titulares de derechos de autor o conexos ha sido suprimida o alterada sin autorización.

b.10 **Venezuela**: el capítulo V —"De los delitos contra el orden económico"— de la LECDI —año 2001— prevé las figuras de apropiación de propiedad intelectual (art. 25)[179] y oferta engañosa (art. 26).[180]

6 | Otras formas de responsabilidad y sanción

La sección del derecho penal material finaliza con el Título 5, "Otras formas de responsabilidad y sanción", constituida por tres artículos en los que se incursiona en temas propios de la parte general del derecho penal.

6.1 | Tentativa y complicidad (art. 11)

En el artículo 11,[181] "Tentativa y complicidad", el primer parágrafo requiere la adopción de reglas de extensión de responsabilidad con relación a los

(179) Su texto: "Apropiación de propiedad intelectual. Quien sin autorización de su propietario y con el fin de obtener algún provecho económico, reproduzca, modifique, copie, distribuya o divulgue un software u otra obra del intelecto que haya obtenido mediante el acceso a cualquier sistema que utilice tecnologías de información, será sancionado con prisión de uno a cinco años y multa de cien a quinientas unidades tributarias".

(180) Su texto: "Oferta engañosa. Toda persona que ofrezca, comercialice o provea de bienes o servicios, mediante el uso de tecnologías de información, y haga alegaciones falsas o atribuya características inciertas a cualquier elemento de dicha oferta, de modo que pueda resultar algún perjuicio para los consumidores, será sancionada con prisión de uno a cinco años y multa de cien a quinientas unidades tributarias, sin perjuicio de la comisión de un delito más grave".

(181) Tiene la siguiente redacción: "Artículo 11 - Tentativa y complicidad

1. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, cualquier acto de complicidad que sea cometido dolosamente y con la intención de favorecer la perpetración de alguna de las infracciones establecidas en los arts. 2 a 10 del presente Convenio.
2. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, la tentativa dolosa de cometer una de las infracciones establecidas en los arts. 3 a 5, 7, 8, 9 (1) a y 9 (1) c del presente Convenio.
3. Las Partes podrán reservarse el derecho de no aplicar, en todo o en parte, el párrafo 2 del presente artículo". Esta propuesta, incluyendo la "inducción", fue reafirmada mediante la Decisión Marco 2005/222/JAI del Consejo, de 24 de febrero de 2005, relativa a los ataques contra los sistemas de información, con esta redacción: "Artículo 5. Inducción, complicidad y tentativa. 1) Cada Estado miembro garantizará que la inducción a los delitos contemplados en los arts. 2, 3 y 4 y la complicidad con ellos sean sancionables como infracciones penales. 2) Cada Estado miembro garantizará que la tentativa de cometer los delitos mencionados en los arts. 2, 3 y 4 sea sancionable como infracción penal. 3) Cada Estado miembro podrá decidir que no se aplique el apart. 2 a las infracciones mencionadas en el art. 2". Fue sustituido por el art. 8

actos de complicidad dolosa y con intención de favorecer la perpetración de alguna de las conductas infractoras anteriores; lo que no provoca niguna necesidad de modificación local en la medida de que todos los códigos latinoamericanos contemplan dispositivos de amplificación típica en materia de participación. El segundo párrafo impulsa el adelantamiento de la intervención penal al momento de perfeccionarse la tentativa dolosa de los tipos previstos en los artículos 3° a 5°, 7° a 9.1.a y 9.1.c; aunque el tercer párrafo prevé la posible reserva total o parcial en este aspecto —no en relación al primero—. Entiendo que la situación es similar a la anterior. Aun cuando, excepcionalmente, en alguna de las legislaciones comparadas se ha optado por incluir en el mismo tipo de la parte especial —así, Paraguay—, la aclaración de su punición a título de tentativa en nuestros códigos; se incorpora, como previsión de la parte general, este otro mecanismo amplificador de la tipicidad al inicio de los actos de ejecución en supuestos en que la consumación no se perfecciona por razones ajenas a la voluntad del agente. Suele también acompañarse de una escala de pena reducida.

6.2 | Responsabilidad de las personas jurídicas (art. 12)

En el artículo 12,[182] "Responsabilidad de las personas jurídicas"; que requiere que se adopten medidas internas que permitan responsabilizar a las personas de existencia ideal por las anteriores infracciones, sin perjuicio de la responsabilidad penal que corresponda a las personas físicas que

de la Directiva 2013/40/UE del Parlamento Europeo y del Consejo de 12 de agosto de 2013 relativa a los ataques contra los sistemas de información, con similar redacción y remisión a sus propios arts. 3 a 7. Vale resaltar que los mencionados arts. 2, 3 y 4 de la DM de 2005, eran equivalentes a los arts. 2, 4 y 5 del Convenio de Budapest, mientras que los arts. 3 a 7 de la Directiva de 2013 se corresponden con los arts. 2 a 6 del CB.

(182) Dice: "Artículo 12 – Responsabilidad de las personas jurídicas

1) Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para permitir que las personas jurídicas puedan ser tenidas por responsables de las infracciones establecidas en el presente Convenio, cuando éstas sean cometidas por una persona física, actuando ya sea a título individual, ya sea como miembro de un órgano de la persona jurídica, que ejerce un poder de dirección en su seno, cuyo origen se encuentre en:
   a. un poder de representación de la persona jurídica;
   b. una autorización para tomar decisiones en nombre de la persona jurídica;
   c. una autorización para ejercer control en el seno de la persona jurídica.
2) Fuera de los casos previstos en el párrafo 1, las Partes adoptarán las medidas necesarias para asegurar que una persona jurídica puede ser tenida por responsable cuando la

las integran; ha evitado todo problema en el nivel nacional habida cuenta que el tercer inciso, respetuoso de los principios jurídicos propios de cada estado signatario, admite su resolución como penal, civil o administrativa. De tal suerte, si bien pueden mediar diferencias en la forma que consideran esta responsabilidad en los distintos países, no hay conflicto con los requerimientos del Convenio.

En relación con lo anterior, Silva Sánchez comenta que un texto como éste no resulta una verdadera novedad en el ámbito de los documentos internacionales, donde pueden encontrarse otros que se refieren con mayor amplitud a los entes ideales y con mayor restricción en cuanto consagran exclusivamente responsabilidad a título penal —artículo 14 del "Corpus Juris", año 1997, o artículo 13, año 2000 —. En este sentido, califica a la previsión del Convenio —en cuanto no "impone" una "naturaleza jurídica"—como consagratoria de un modelo relativamente abierto de responsabilidad directa y acumulativa —no subsidiaria y alternativa—, de las personas jurídicas.(183)

ausencia de vigilancia o de control por parte de cualquier persona física mencionada en el párrafo 1 haya permitido la comisión de las infracciones descritas en el párrafo 1 a través de una persona física que actúa bajo autorización de la persona jurídica.

3) La responsabilidad de la persona jurídica podrá resolverse en sede penal, civil o administrativa, dependiendo de los principios jurídicos propios del Estado.
4) Esta responsabilidad se establecerá sin perjuicio de la responsabilidad penal de las personas físicas que hayan cometido la infracción".

La propuesta fue reafirmada mediante la DM 2005/222/JAI del Consejo, de 24 de febrero de 2005, relativa a los ataques contra los sistemas de información, con esta redacción: "Artículo 8. Responsabilidad de las personas jurídicas. 1) Cada Estado miembro adoptará las medidas necesarias para que a las personas jurídicas se les puedan exigir responsabilidades por las infracciones mencionadas en los arts. 2, 3, 4 y 5, cuando dichas infracciones sean cometidas en su beneficio por cualquier persona, actuando a título particular o como parte de un órgano de la persona jurídica, que ostente un cargo directivo en el seno de dicha persona jurídica basado en: a) un poder de representación de dicha persona jurídica, o b) una autoridad para tomar decisiones en nombre de dicha persona jurídica, o c) una autoridad para ejercer un control en el seno de dicha persona jurídica. 2) Sin perjuicio de los casos previstos en el apartado 1, los Estados miembros garantizarán que a las personas jurídicas se les puedan exigir responsabilidades cuando la falta de vigilancia o control por parte de alguna de las personas a que se refiere el apart. 1 haya hecho posible que una persona sometida a su autoridad cometa las infracciones mencionadas en los arts. 2, 3, 4 y 5 en beneficio de esa persona jurídica. 3) La responsabilidad de las personas jurídicas en virtud de los aparts. 1 y 2 se entenderá sin perjuicio de la incoación de acciones penales contra las personas físicas que sean autores, incitadores o cómplices en la comisión de las infracciones mencionadas en los arts. 2, 3, 4 y 5". Fue sustituido por el art. 10 de la Directiva 2013/40/UE del Parlamento Europeo y del Consejo de 12 de agosto de 2013 relativa a los ataques contra los sistemas de información, con similar redacción y remisión a sus propios arts. 3 a 8.

(183) Silva Sánchez, Jesús-María, "La responsabilidad penal de las personas jurídicas en el Convenio del Consejo de Europa sobre cibercriminalidad",en Morales García (dir.), *Delin-*

Puede anotarse que la ley especial venezolana del año 2001 —sin dudas, la más extensa en la región— incorporó una previsión expresa relativa a la responsabilidad de las personas jurídicas: su art. 5.(184) En la base se encontraría el reconocimiento de la singular importancia que tienen las diferentes clases de prestadores de servicio en la estructura y configuración de la red telemática. No son otra cosa que grandes empresas que se benefician y, a la vez, tienen una cierta cuota de responsabilidad —co-responsabilidad— en el control de asuntos, objetos o servicios ofrecidos cotidianamente por Internet. Esto obliga, al decir de Aboso y Zapata, a replantearse la responsabilidad penal de las personas de existencia ideal, en muchos países sistemáticamente negada al calor del aforismo romano *societas delinquere non potest*.(185)

6.3 | Sanciones y medidas (art. 13)

Finalmente, el artículo 13(186), "Sanciones y medidas", tal como se enfatizó en la introducción, brinda pautas genéricas acerca del tipo de sanciones que los estados deben adoptar para punir las infracciones penales des-

cuencia Informática. Problemas de responsabilidad, Cuadernos de Derecho Judicial IX-2002, Consejo General del Poder Judicial, Madrid, 2002, pp. 116/117 y 120/121.

(184) Dice: "Responsabilidad de las personas jurídicas. Cuando los delitos previstos en esta Ley fuesen cometidos por los gerentes, administradores, directores o dependientes de una persona jurídica, actuando en su nombre o representación, éstos responderán de acuerdo con su participación culpable. La persona jurídica será sancionada en los términos previstos en esta Ley, en los casos en que el hecho punible haya sido cometido por decisión de sus órganos, en el ámbito de su actividad, con sus recursos sociales o en su interés exclusivo o preferente".

(185) Aboso, Gustavo E.; Zapata, María F., *Cibercriminalidad y derecho penal*, Bs. As., B de F, 2006, p. 211.

(186) Su texto: "Artículo 13 – Sanciones y medidas

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

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

Con mayor detalle tanto respecto de personas físicas como jurídicas y endureciendo las penas, la propuesta fue reafirmada mediante la DM 2005/222/JAI del Consejo, de 24 de febrero de 2005, a través de sus arts. 6, 7 y 9, que llega a incluir escalas de sanciones de privación de libertad y circunstancias agravantes en algunos casos. Fueron sustituidos por los arts. 9 (que fusiona y amplía los mencionados 6 y 7 de la DM) y 11 de la Directiva 2013/40/UE del Parlamento Europeo y del Consejo de 12 de agosto de 2013 relativa a los ataques contra los sistemas de información.

criptas en los artículos 2° a 11. Éstas deben ser efectivas, proporcionadas y disuasorias. Se admiten las penas privativas de libertad con relación a las personas físicas (primer párrafo), así como las pecuniarias respecto de las personas jurídicas (segundo párrafo).

En cuanto a las últimas como sujeto de sanción, Silva Sánchez destaca que la utilización de este término sugiere que se prescribe un modelo de responsabilidad más allá de lo estrictamente reparatorio. Por lo que concluye que un modelo de exclusiva responsabilidad civil compensatoria no cumpliría las exigencias del Convenio. Así, estima que dicho Convenio situaría el mínimo de lo "proporcionado, efectivo y disuasorio" en el empleo, al menos, de una indemnización sancionatoria —*punitive damages*—.[187]

Limito la transcripción a los ahora vigentes: "Artículo 9. Sanciones. 1) Los Estados miembros adoptarán las medidas necesarias para garantizar que las infracciones mencionadas en los arts. 3 a 8 se castiguen con penas efectivas, proporcionadas y disuasorias. 2) Los Estados miembros adoptarán las medidas necesarias para garantizar que las infracciones mencionadas en los arts. 3 a 7 se castiguen con sanción máxima de privación de libertad igual o superior a dos años, al menos en los casos que no sean de menor gravedad. 3) Los Estados miembros adoptarán las medidas necesarias para garantizar que, cuando se hayan afectado a un número significativo de sistemas de información o cuando para cometerlas se haya utilizado uno de los instrumentos a que se refiere el art. 7, las infracciones mencionadas en los arts. 4 y 5, se castiguen con una sanción máxima de privación de libertad de al menos tres años. 4) Los Estados miembros adoptarán las medidas necesarias para garantizar que las infracciones mencionadas en los arts. 4 y 5 se castiguen con una sanción máxima de privación de libertad de al menos cinco años cuando: a) se cometan en el contexto de una organización delictiva con arreglo a la Decisión marco 2008/841/JAI, con independencia del nivel de la sanción que se establezca en la misma; b) causen daños graves, o c) se cometan contra el sistema de información de una infraestructura crítica. 5) Los Estados miembros tomarán las medidas necesarias para garantizar que, cuando las infracciones a que se refieren los arts. 4 y 5 sean cometidas utilizando ilícitamente datos de carácter personal de otra persona con la finalidad de ganar la confianza de un tercero, causando así daños al propietario legítimo de la identidad, ello pueda ser considerado, de conformidad con el Derecho nacional, como circunstancia agravante, a menos que tal circunstancia ya esté contemplada con otra infracción que sea sancionable con arreglo al Derecho nacional"; y "Art. 11. Sanciones contra las personas jurídicas. 1) Los Estados miembros adoptarán las medidas necesarias para garantizar que a la persona jurídica considerada responsable en virtud de lo dispuesto en el art. 10, apart. 1, le sean impuestas sanciones efectivas, proporcionadas y disuasorias, que incluirán multas de carácter penal o de otro tipo, y entre las que podrán incluir otras sanciones como: a) exclusión del disfrute de ventajas o ayudas públicas; b) inhabilitación temporal o permanente para el ejercicio de actividades comerciales; c) vigilancia judicial; d) medida judicial de liquidación; e) cierre temporal o definitivo de los establecimientos utilizados para cometer la infracción. 2) Los Estados miembros adoptarán las medidas necesarias para garantizar que a la persona jurídica considerada responsable en virtud de lo dispuesto en el art. 10, apart. 2, le sean impuestas sanciones o medidas efectivas, proporcionadas y disuasorias".

(187) Sánchez, *op. cit.*, p. 122.

Un rápido repaso de la cuantiosa normativa a la que nos referimos en este trabajo revela que, lejos de ser una excepción, la pena privativa de libertad —con distintas denominaciones y extensión; prisión, reclusión, detención, presidio— es la más asiduamente utilizada; ya sea sola o conjunta con la de multa o con la de inhabilitación especial, o alternativa con la de multa o la de prestación de servicios comunitarios. Salvo en el caso del CP de Paraguay, que responde con claridad al modelo alemán y, por lo tanto, sólo establece el tope máximo de privación de libertad posible; en los demás las escalas son fijadas con un mínimo y máximo determinados o mediante una regla de determinación derivada —así, el CP de Chile, de mayor semejanza con el sistema español—.

En muy pocos casos se prevé sólo multa. Esta pena a veces se expresa directamente en una cantidad variable de moneda de curso legal del país de que se trate y, en otras, remite a alguna otra unidad determinativa. Por ejemplo, "unidades tributarias", "unidades reajustables", "salarios mínimos legales mensuales" o "días-multa".

7 | Recapitulación final

Sin perjuicio de insistir en todas las prevenciones formuladas al inicio, la tabla que seguidamente se incorpora permite visualizar de un modo claro y sencillo el resultado del ejercicio comparativo entre el Convenio de Budapest y las legislaciones de los países miembros plenos o asociados del Mercosur.

Los encasillamientos propuestos son tendenciales, basados particularmente en la adopción de reformas o modificaciones legales que incorporaron nuevas tipicidades o actualizaron otras anteriormente vigentes. Pero ello no descarta la posibilidad de que la carencia u omisión de normativa de moderna factura no se traduzca en forma directa en atipicidad ya que, en muchos casos, es factible que por vía interpretativa de la redacción de tipos previos a la irrupción de las TIC se dé solución a nivel local a eventuales lagunas de punición.

Esta última situación puede entonces operar como una suerte de efecto ralentizador de la actividad legislativa tendiente a armonizar el derecho interno a la propuesta convencional.

En principio, puede decirse que Argentina, Paraguay y Venezuela no ofrecerían déficit de tipificación alguno en confronte con las demandas de Budapest. En el otro extremo, Bolivia y Uruguay serían los Estados que necesitarían una urgente actualización para entrar en sintónica armonía con los restantes. En ambos hay proyectos de reforma en consideración en la actualidad.

a. No obstante, como primera observación, es dable concluir que, la región del Mercosur no ofrece mayores problemas para su integración con los restantes signatarios del Convenio europeo en materia de derecho penal material.

La síntesis gráfica de la comparación entre la Sección 1 del II del Convenio de Budapest y las legislaciones de la región queda expresada del siguiente modo:

CUADRO 1. CONVENIO DE BUDAPEST Y LEGISLACIONES COMPARADAS. SÍNTESIS DE COMPARACIÓN

Budapest	Art. 2	Art. 3	Art. 4	Art. 5	Art. 6	Art. 7	Art. 8	Art. 9	Art. 10
Argentina	sí	sí	sí	sí	sí	sí	sí	sí	sí
Bolivia	sí	no	sí	no	no	no	si	no	sí
Brasil	no	sí	sí	sí	si	sí	no	si	sí
Chile	no	sí	si	no	no	sí	sí	sí	sí
Colombia	sí	sí	sí	sí	sí	no	sí	sí	sí
Ecuador	sí	sí	sí	sí	no	no	sí	sí	sí
Paraguay	sí	sí	sí	sí	sí	sí	sí	sí	sí
Perú	sí	sí	sí	sí	sí	no	sí	sí	sí
Uruguay	no	sí	no	no	no	sí	no	sí	sí
Venezuela	sí	sí	sí	sí	sí	sí	sí	sí	sí

Referencias: Art. 2= Acceso ilícito; Art. 3= Interceptación ilícita; Art. 4= Atentados contra la integridad de los datos; Art. 5= Atentados contra la integridad del sistema; Art. 6= Abuso de equipos e instrumentos técnicos; Art. 7= Falsedad informática; Art. 8= Estafa informática; Art. 9= Infracciones relativas a la pornografía infantil; Art. 10= Infracciones vinculadas a los atentados a la propiedad intelectual y derechos afines.

b. Con relación a la forma en que se penan las infracciones contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas in-

formáticos —Título 1—, si bien resulta clara la uniformidad en cuanto al uso de la pena privativa de libertad como principal modo de respuesta; puede advertirse rápidamente la diversidad con que en general se recibe el genérico mandato del art. 13: las sanciones han de ser "efectivas, proporcionadas y disuasorias" habida cuenta las disímiles escalas conminadas en abstracto, así como las variantes en alternatividad o conjunción con otras modalidades de penas. Con la misma advertencia del punto anterior acerca de volcarse una respuesta tendencial por las razones allí expuestas, pueden destacarse las siguientes observaciones particulares:

b.1 Acceso ilícito (art. 2°): Bolivia es el único que no admite pena privativa de libertad. En cambio, prevé penas de prestación de trabajo o multa. Todos los demás contemplan pena privativa de libertad. Argentina es el único que la prevé en forma exclusiva. Paraguay admite la posibilidad alternativa de multa. Perú admitía la alternativa de prestación de servicios comunitarios, pero con la ley 30.096 de octubre de 2013 ahora mantiene la pena privativa de libertad y días multa como sanción conjunta. Finalmente; Colombia, Ecuador y Venezuela prevén aplicación conjunta de prisión y multa.

b.2 Interceptación ilícita (art. 3°): en este caso, todos contemplan pena privativa de libertad. Argentina, Chile, Colombia, Perú y Uruguay, de forma exclusiva. Paraguay admite la posibilidad alternativa de multa. En cambio, Brasil, Ecuador y Venezuela prevén aplicación conjunta de prisión y multa.

b.3 Atentados contra la integridad de los datos (art. 4°): nuevamente Bolivia es el único que no admite pena privativa de libertad sino que prevé las de prestación de trabajo o multa. Los demás contemplan pena privativa de libertad. Argentina y Chile, de forma exclusiva. Paraguay admite la posibilidad alternativa de multa. Brasil, en algunos tipos, admite la multa conjunta y, en otros, alternativa. Por último, Colombia, Ecuador, Perú y Venezuela prevén aplicación conjunta de prisión y multa.

b.4 Atentados contra la integridad del sistema (art. 5°): respecto de esta conducta, todos contemplan pena privativa de libertad. Argentina lo hace de forma exclusiva, mientras que Paraguay admite la posibilidad alternativa de multa. Por su lado, Brasil, Colombia, Ecuador, Perú y Venezuela prevén aplicación conjunta de prisión y multa.

b.5 Abuso de equipos e instrumentos técnicos (art. 6°): nuevamente todos prevén como sanción la pena privativa de libertad, Argentina es el único que lo hace en forma exclusiva y Paraguay admite la posibilidad alternativa de multa. Brasil, Colombia, Perú y Venezuela prevén aplicación conjunta de prisión y multa.

Lo expuesto se sintetiza gráficamente en el cuadro que sigue:

CUADRO 2. PENAS CONTRA LAS INFRACCIONES. SINTESÍS GRÁFICA. ARTS. 2 A 6

Budapest	Art. 2	Art. 3	Art. 4	Art. 5	Art. 6
Argentina	P 15D a 2A	P 15D a 1A	P 15D a 6A	P 6M a 2A	P 15D a 1A
Bolivia	pT hasta 1A o M hasta 200D	no	PT hasta 1A o M hasta 200D	no	no
Brasil	no	P 2 a 4A y M	P 1M a 12A y/o M	P 1M a 3A y M	P 3M a 1A y M
Chile	no	P menor grado mín. a medio	P menor grado mín. a máximo	no	no
Colombia	P 48 a 96M y M 100 a 1000S	P 36 a 72M	P 48 a 96M y M 100 a 1000S	P 48 a 96M y M 100 a 1000S	P 48 a 96M y M 100 a 1000S
Ecuador	P 1 a 3A y M 1000 a 1500 u$s	P 2M a 9A y M 1000 a 10000 u$s	P 6M a 6A y M 60 a 600 u$s	P 8M a 4A y M 200 a 600 u$s	no
Paraguay	P hasta 3A o M	P hasta 3A o M	P hasta 5A o M	P hasta 5A o M	P hasta 1A o M
Peru	P 1A a 4A y 30 a 90 DM	P 3A hasta 10A	P 3A a 6A y 80 a 120 DM	P 3A a 6A y 80 a 120 DM	P 1A a 4A y 20 a 60 DM
Uruguay	no	P 3M a 3A	no	no	no
Venezuela	P 1 a 5A y M 10 a 50 UT	P 3 a 6A y M 300 a 600 UT	P 2 a 10A y M 200 a 1000 UT	P 2 a 10A y M 200 a 1000 UT	P 3 a 6A y M 300 a 600 UT

Aclaración: en el caso de países en los que concurren varios tipos a cubrir el pertinente artículo del Convenio de Budapest, la escala se formó con el mínimo menor y el máximo mayor posibles; considerando tipos básicos y especiales, y sin incluir agravantes genéricos. Tampoco se incorporaron ni consideraron las muy comunes sanciones de inhabilitación cuando el hecho es cometido por funcionario o persona encargada de la custodia, o el decomiso de los elementos del delito.

Referencias: Art. 2°= Acceso ilícito; Art. 3°= Interceptación ilícita; Art. 4°= Atentados contra la integridad de los datos; Art. 5°= Atentados contra la integridad del sistema; Art. 6°= Abuso de equipos e instrumentos técnicos.

Abreviaturas: P= privación de libertad (prisión, reclusión, detención, presidio, penitenciaría); "x" D= cantidad de días; "x" M= cantidad de meses; "x" A= cantidad de años; PT= prestación de trabajo; M= multa; DM= días-multa; "x" S= cantidad de salarios; "x" J= cantidad de jornadas; UT= unidades tributarias; UVC= unidad de valor constante.

c. Con relación a la forma en que se penan las infracciones informáticas, de contenido o contra la propiedad intelectual y derechos afines (Títulos 2, 3, y 4), reiterando la advertencia genérica, se mantiene idéntica ob-

servación en cuanto a la uniformidad en el uso de la pena privativa de libertad como principal modo de respuesta y diversidad para recibir el genérico mandato del art. 13 en orden a que las sanciones han de ser "efectivas, proporcionadas y disuasorias". Sentado ello, pueden destacarse las siguientes particularidades:

c.1 Falsedad informática (art. 7°): todos los países contemplan penas con privación de libertad. Argentina,[188] Chile y Uruguay lo prevén en forma exclusiva. Paraguay admite la posibilidad alternativa de multa. Finalmente, Brasil y Venezuela prevén la aplicación conjunta de prisión y multa.

c.2 Estafa informática (art. 8°): nuevamente todos contemplan la pena privativa de libertad. Argentina y Chile, de forma exclusiva; Paraguay admite la posibilidad alternativa de multa. Por último; Bolivia, Colombia, Ecuador y Venezuela prevén la aplicación conjunta de prisión y multa.

c.3 Infracciones relativas a la pornografía infantil (art. 9°): se mantiene la nota de uso por todos de la pena privativa de libertad que, en este caso, es prevista en forma exclusiva por Argentina, Chile, Ecuador y Uruguay. Paraguay admite la posibilidad alternativa de multa. Brasil, Colombia, Perú y Venezuela prevén aplicar en conjunto prisión y multa.

c.4 Infracciones vinculadas a los atentados a la propiedad intelectual y derechos afines (art. 10): todos prevén la pena privativa de libertad. Argentina y Uruguay en forma exclusiva, en tanto Paraguay admite la posibilidad alternativa de multa. En cambio, la aplicación conjunta de prisión y multa es la opción de Bolivia, Brasil, Chile, Colombia, Ecuador y Venezuela.

CUADRO 3. PENAS CONTRA LAS INFRACCIONES. SINTESÍS GRÁFICA. ARTS. 7 A 10

Budapest	Art. 7	Art. 8	Art. 9	Art. 10
Argentina	P 1 a 6A	P 1M a 6A	P 1M a 4A	P 1M a 6ª
Bolivia	no	P 1 a 5A y M 60 a 200D	no	P 3M a 2A y M 30 a 60D
Brasil	P 1 a 5A y M	no	P 3 a 8A y M	P 6M a 4A y M
Chile	P menor en cualquier grado	P menor en cualquier grado	P menor grado med. a máx.	P menor grado mín. y M 5 a 50 UT
Colombia	no	P 48 a 120M y M 200 a 1500S	P 10 a 20A y M 150 a 1500S	P 32 a 90M y M 26,66 a 300S

(188) Se tomó como referencia la escala del art. 292 del CP.

Budapest	Art. 7	Art. 8	Art. 9	Art. 10
Ecuador	no	P 6M a 5A y M 500 a 2000 u$s	P de 6 a 9A	P 3M a 3A y M 500 a 5000 UVC
Paraguay	P hasta 5A o M	P hasta 5A o M	P hasta 5A o M	P h. 3A o M
Peru	no	P 3A a 10A y 60 a 140 DM	P 6A a 12A y 120 a 365DM	P hasta 6A y 10 a 120DM
Uruguay	P 3 meses a 10 años	no	P 6 meses a 12 años	P 3 meses a 3 años
Venezuela	P 3 a 6 años y M 300 a 600 UT	P 1 a 7 años y M 10 a 700 UT	P 2 a 8 años y M 200 a 800 UT	P 1 a 5 años y M 100 a 500 UT

Aclaración: en el caso de países en los que concurren varios tipos a cubrir el pertinente artículo del Convenio de Budapest, la escala se formó con el mínimo menor y el máximo mayor posibles, considerando tipos básicos y especiales y sin incluir agravantes genéricos. Tampoco se incorporaron ni consideraron las muy comunes sanciones de inhabilitación cuando el hecho es cometido por funcionario o persona encargada de la custodia, o el decomiso de los elementos del delito.

Referencias: Art. 7° = Falsedad informática; Art. 8° = Estafa informática; Art. 9° = Infracciones relativas a la pornografía infantil; Art. 10 = Infracciones vinculadas a los atentados a la propiedad intelectual y derechos afines;

Abreviaturas: "x" D= cantidad de días; "x" M= cantidad de meses; "x" A= cantidad de años; PT= prestación de trabajo; M= multa; DM= días-multa; "x" S= cantidad de salarios; "x" J= cantidad de jornadas; UT= unidades tributarias; UVC= unidad de valor constante.

c. Poco más de una década después del Convenio de Budapest, comienza a surgir el interés en que las legislaciones nacionales incorporen nuevas tipicidades o refuercen las anteriores. Por caso, en la Unión Europea la "Directiva 2013/40/UE del Parlamento y del Consejo de 12 de agosto de 2013 relativa a los ataques contra los sistemas de información", respecto del robo o suplantación de identidad digital.[189] También se propulsa la incorporación de figuras que capten con más precisión, entre otras conductas dis-

(189) En Argentina existe un proyecto con trámite parlamentario que fue presentado el 15 de mayo de 2012 por la senadora Higonet (Exp. S N° 1312/12). A partir de éste se incorporaría como artículo 138 *bis* del CP con el siguiente texto: "Será reprimido con prisión de 6 (seis) meses a 3 (tres) años o multa de pesos veinte mil a pesos doscientos mil, el que sin consentimiento, adquiriere, tuviere en posesión, transfiriere, creare o utilizare la identidad de una persona física o jurídica que no le pertenezca, a través de internet o cualquier otro medio electrónico, y con la intención de dañar, extorsionar, defraudar, injuriar o amenazar a otra persona u obtener beneficio para sí o para terceros".

valiosas; el *grooming*, el *ciberstalking* o el *ciberbullying*. Serían temas para seguir pensando el fenómeno expansivo del derecho penal. Del otro lado queda sobre todo la necesidad de reflexionar acerca de la racionalidad de seguir usándolo para conductas que tienen un alto grado de aceptación y son muy extendidas socialmente, cuya dañosidad básicamente es de orden patrimonial y que, por lo tanto, bien pudieran ser devueltas al ámbito civil, comercial y, si se quiere mantener una cierta cuota de poder punitivo al derecho sancionador administrativo o contravencional. Me refiero a la actividad *cuasi bagatelar* de agentes como los "manteros" —como se les llama en Latinoamérica— o "top manta/top mochila" —en España—, así como la tan frecuente de intercambio de archivos *on line*.(190)

(190) Este problema ha sido perfectamente captado por Javier A. De Luca, titular de la Fiscalía General N° 4 ante la Cámara Nacional de Casación Penal, en su dictamen N° 7868 en causa "Andrade, Luz María s/recurso de queja", causa N° 16.914 de la Sala I, al desistir del recurso incoado en la etapa previa. El supuesto de hecho comprometía el secuestro de un total de 33 CD de música y 102 películas y videojuegos identificados precariamente todos con fotocopias de los originales, que la imputada comerciaba en la vía pública. Al fundar el desistimiento apuntó que la conducta investigada no constituía delito infractorio a la Ley de Marcas (N° 22.362), por la insignificante lesión al bien jurídico protegida por ésta. Vale aclarar que la presunta infracción a la Ley de Propiedad Intelectual corresponde al fuero común, no al federal, por lo que no entró en consideración en el caso, según se precisa en el propio dictamen. No puedo dejar de señalar que este desdoblamiento es incorrecto y lo que hubiera correspondido es que el fuero de excepción, es decir el federal, se hubiera hecho cargo de toda la imputación y no mantener esta ficcionada separación de lo que no es más que el mismo hecho visto desde dos tipicidades que, a todo evento, no constituiría más que un supuesto de concursalidad aparente.
Por lo demás, criticó De Luca abiertamente la actividad policial diciendo: "La acción de las autoridades en casos como el presente, se limita a la detección y represión de los llamados 'manteros' o vendedores ambulantes de objetos falsificados, a sacarlos de circulación e incautarse de la mercadería, sin realizar el más mínimo esfuerzo pesquisitivo para proseguir hacia arriba en la línea o pirámide delictiva y, así, descubrir y desbaratar a las organizaciones que están detrás de la producción de estos productos imitados que, precisamente, emplean a personas de bajos recursos económicos, sociales y culturales para llevar adelante su comercialización ilegal. Todo se reduce a lo mismo que ha ocurrido con la llamada 'lucha contra las drogas', donde se ha teorizado inclusivo que debe perseguirse a los consumidores porque, al ser los últimos eslabones de la cadena delictiva, con su represión se 'atraerán' (tirando de esa cadena, valga la redundancia) hacia nosotros a los productores y comercializadores. Si esto no fuese un asunto muy serio, realmente asombra por su candidez".

Los denominados "delitos informáticos" y la estructura general del Anteproyecto de Código Penal

por **EDUARDO E. ROSENDE**[1]

I | Aclaración previa

Durante el año 2012, junto con otros colegas de la especialidad, tuve la suerte de ser invitado por los miembros de la Comisión para la Elaboración del Proyecto de Ley de Reforma, Actualización e Integración del Código Penal de la Nación (decreto 678/12), para discutir e intercambiar opiniones acerca del estado de la legislación penal en materia de hechos relacionados con el procesamiento automático de la información.

En esas jornadas surgieron distintas ideas de recambio para la plataforma legal que había ido materializándose a lo largo de los últimos años y que culminó con la ley 26.388, cuyo contenido fue motivo de análisis y críticas en varias ocasiones anteriores.

El objetivo de estas páginas es brindar un cuadro de situación acerca del estudio previo de la parte general del Código Penal actual, las ideas opor-

(1) Abogado, especialista en Derecho Penal. Jefe de Trabajos Prácticos del Departamento de Derecho Penal y Criminología de la UBA y de la Universidad John F. Kennedy. Profesionalmente se desempeña como funcionario del Ministerio Público Fiscal de la Nación.

tunamente expresadas a la comisión y, finalmente, esbozar los resultados arrojados por el Anteproyecto en esta materia tan peculiar y específica, relacionada con los **delitos informáticos**.

2 | Análisis de las modificaciones

2.1 | Firma electrónica y firma digital: error de la asimetría en la protección penal

El actual proyecto de reforma integral, mantiene la letra del código actual en este sentido, y contempla la siguiente definición:

> "k) Los términos "firma" y "suscripción" comprenden la firma digital, la creación de una firma digital o firmar digitalmente. Los términos "documento", "instrumento privado" y "certificado" comprenden al documento digital firmado digitalmente". (art. 63, inc. k)

Dicho párrafo es la consecuencia del repaso de las leyes 25.326, 25.506 y 26.388. Lamentablemente, el Anteproyecto mantiene singulares e importantes problemas:

La ley no ha otorgado protección a los documentos firmados electrónicamente, concentrando la cobertura penal en forma exclusiva solo para aquellos documentos digitales que hayan sido firmados con la denominada firma digital.

Dicho punto, si bien discutible desde una perspectiva de política criminal, parece desacertado en razón de que la única diferencia que reviste la firma electrónica de la digital resulta ser meramente legal. Desde lo técnico, ambas estructuras pueden resultar idénticas en cuanto a seguridad, confidencialidad y fijación de autoría en el almacenamiento y trasmisión de datos.

Por ello, ambos métodos de firmado son utilizados en forma masiva en el mundo, y si bien la firma digital cuenta con más estructura y soporte, la firma electrónica tiene un costo muchísimo menor en su uso y, por lo tanto, podría resultar más popular y masiva. Tal aspecto de la estructura de la firma electrónica que, en sentido lato, incluye a la firma digital (art. 2) y la

firma electrónica (art. 5) de nuestra Ley de Firma Digital —ley 25.506— que contempla y brinda la base legal a los dos procesos de firmado en forma correcta.

No existe razón, pues, para no trabajar en forma conjunta ambas formas de firmado en el ámbito penal; a modo de analogía, podría decirse que la única diferencia entre un sistema y otro es la confianza depositada por el Estado Nacional en una Entidad Certificante específica, mientras que los efectos lesivos a derechos de terceros pueden originarse en la falsificación de cualquiera de estos sistemas.

En su momento fue acercada la propuesta de modificar parte del inciso, para dejarlo con la siguiente redacción: "k) Los términos 'firma' y 'suscripción' comprenden la firma digital o electrónica, la creación de una firma digital o electrónica, o firmar digitalmente o electrónicamente." Lamentablemente, tal propuesta no tuvo favorable receptación.

Sin embargo, para finalizar este punto, debemos remarcar el acierto, en cuanto a taxatividad de la ley penal se refiere, en el desarrollo y especificación del concepto de dato informático, a través de la delimitación de su contenido para la interpretación penal, que abarcará cualquiera de sus atributos y no meramente el borrado o eliminación total o parcial, al efectuarse específicas referencias a

> "los datos relativos al tráfico, entendiendo como tales todos los relativos a una comunicación realizada por medio de un sistema informático, generados por este último en tanto que elemento de la cadena de comunicación, y que indican el origen, el destino, la ruta, la hora, la fecha, el tamaño y la duración de la comunicación o el tipo de servicio subyacente".

2.2 | El principal defecto del Código Penal aún se mantiene

Nos referimos a que la falsificación de documentos públicos firmados digitalmente no encuadraría en el concepto de instrumento público del art. 292 del Código Penal; es decir, afirmamos la atipicidad completa de la falsificación de ese tipo de documentos digitales.

Este problema se originó en una confusa técnica legislativa que seguramente dará lugar a interpretaciones contrarias al sentido de las normas penales ya vigentes y cuya relaboración no ha corregido este defecto: se trata de la posibilidad de haber dejado como acciones atípicas aquellas conductas relacionadas con la falsificación de instrumentos públicos.

Recordemos que la ley de firma digital resulta clara (al menos en sus primeros y centrales artículos) en cuanto a la actualización tecnológica que ha venido de la mano de la informatización de nuestra vida y la creación de documentos intangibles.

Sin embargo, la aclaración de conceptos introducidas al Código Penal por el art. 51 de la citada ley y no modificada en su esencia por la ley 26.388, originará en la aplicación jurisprudencial un problema de cabal importancia: si el documento digital firmado digitalmente comprende al instrumento privado, el documento digital (sin importar que sean públicos —art. 979 del CC— o privados) es equiparable únicamente a los instrumentos privados y no a los instrumentos públicos aun cuando estos estén firmados digitalmente por un funcionario público autorizado; por ello, existiría la posibilidad, más que probable, de darse la atipicidad de la conducta en los términos del art. 292 del CP.

Por esto, en su momento se sugirió la modificación de dicha redacción para que el término documento sea definido en los mismos términos del art. 6 de la ley 24.051, y que la frase "documento digital firmado digital o electrónicamente" sea comprensivo de los términos instrumento público o privado según sea el caso (art. 292 del CP actual o 287.1 del proyecto de reforma bajo análisis), el cual debería haber dicho: "Los documentos digitales y certificados acompañados por firma digital o electrónica son equiparables en todos sus efectos legales a los términos instrumento público o privado según sea el caso".

Recordemos en este sentido que, conforme la actual redacción del Anteproyecto, en el Título X "Significación de conceptos empleados en el código", art. 63, inc 4.k) dice: "Los términos 'firma' y 'suscripción' comprenden la firma digital, la creación de una firma digital o firmar digitalmente. Los términos 'documento', 'instrumento privado' y 'certificado' comprenden al documento digital firmado digitalmente".

Ello es una abierta contradicción pues la raíz sobre la que está construida toda la estructura de la firma digital es el certificado raíz emitido por la autoridad central constituida legalmente que, para nuestro caso, es la Jefatura de Gabinete de Ministros (Autoridad certificante de la Administración Pública Nacional). Dicho certificado, conforme la letra actual de nuestra ley, debe ser considerado como un instrumento privado y no como lo que realmente es: un documento emitido por una autoridad en el ejercicio de su función pública (art. 979 CC).

Entonces, la adulteración, la falsificación o la eliminación de dicho certificado, o de cualquier otro certificado firmando por cualquier ministerio, organismo público (ANSES, AFIP, y otros), en los términos del Código Penal y del actual Anteproyecto, solo podrían ser consideradas, en el mejor de los casos, como instrumentos privados.

Ello nos lleva a afirmar que si los certificados digitales emitidos por organismos públicos relacionados con la administración de Justicia (CSJN, Ministerio Público de la Nación, entre otros) son de naturaleza privada, no podría afirmarse por lógica consecuencia que la orden de allanamiento firmada digitalmente por un juez o un fiscal, o cualquiera de sus resoluciones o dictámenes pueda constituir, en los términos del art. 287 del Anteproyecto, un instrumento público.

Por eso, al estar a tiempo de enmendar dicho error, insistimos en que resulta indispensable esta modificación.

2.3 | Del ejercicio de las acciones

Con la entrada en vigencia de la ley 26.388 se actualizó el Código Penal en cuanto a los delitos de violación de secretos y la privacidad, agregándose también nuevas figuras penales.

Sin embargo, al efectuarse esas modificaciones no se tuvieron en cuenta las distintas clases de acciones penales que existen en nuestro sistema, planteándose así, en casos jurisprudenciales, distintos problemas para avanzar en investigaciones frente a hechos que tenían como sujetos activos a funcionarios públicos o cuando las conductas lesivas tenían como objetivos de ataque a sistemas informáticos públicos.

La situación generó que se lleguen a declarar, por distintos tribunales, la nulidad de todo lo actuado en causas donde el Ministerio Público Fiscal actuó de oficio frente a funcionarios relacionados con hechos de este tipo, instando la acción pública cuando ésta, de conformidad con las disposiciones del art. 71 y siguientes del Código Penal, debía ser ejercida mediante querella criminal por el particular.

Entendemos, por diferentes motivos que son objetos de trabajos ya publicados y citados, que ello debería ser tenido en cuenta para establecer que todo hecho cometido por funcionarios públicos en ejercicio de sus cargos o contra bases de datos públicas del Estado, constituyen actos sometidos a la persecución oficial.

Por ello, en su momento se había acercado una propuesta de modificar lo que era el art. 45 del proyecto de la siguiente forma:

"Acciones privadas. Son acciones privadas las que nacen de los siguientes delitos:

a. Delitos contra el honor (arts. 115, 116, 118, 119 y 122);

b. Violación de secretos (144 de este Código), salvo en los siguientes casos: los del art. 145 de este Código; cuando en el hecho haya podido participar un funcionario público en el marco de su competencia, conforme objetivos y razonables indicios al momento de efectuarse la denuncia penal; o cuando las conductas sean realizadas contra sistemas informáticos públicos o de propiedad pública; o en actos que vulneren al momento de iniciarse la acción la privacidad de un grupo amplio e indeterminado de personas.

c. Violación de domicilio (…)".

No obstante, por las particularidades que tiene el Anteproyecto en un sentido más global, se optó por otra forma de regulación de las acciones a través de su correlación con los distintos tipos penales en juego. Más allá de sostener que nuestra propuesta es mucho más clara para evitar que las acciones ilícitas de funcionarios públicos encuentren recovecos de impunidad en la letra de la ley, lo cierto es que la actual regulación que ha hecho el Anteproyecto, ha producido un notable avance en este sentido pues, en cuanto a los delitos contra la privacidad, solo han quedado como de acción privada aquellos establecidos en los artículos 122 inc.1, 123 inc.1 y 123 inc. 3, aparts. a y c); es decir aquellas conductas que no giran en relación a la función pública. Además, en el hipotético caso de un funcionario público que

participe como sujeto activo del hecho, se entraría de lleno en la hipótesis del art. 120 inc. 2 o 122 inc. 2, que resultan ser delitos de acción pública.

También son acertadas las disposiciones relativas a las figuras penales contenidas en el art. 123 del Anteproyecto, en cuanto a su relación con el ejercicio de las acciones, pues ha previsto como de acción privada el acceso o modificación de bases de datos y otorgando oficiosidad a la revelación o uso de dichas bases, para de esa forma evitar la atomización de procedimientos en base a las acciones que cada uno de los afectados pudiera iniciar.

Sin embargo, con respecto al ejercicio de la acción en los casos del art. 123 inc. 3, aparts. a y c) no se ha aclarado ni en la parte general ni en las figuras específicas, quién resultará el titular de dicha acción, pues conforme el bien jurídico afectado, solo podría ser aquel cuya privacidad es afectada por los datos contenidos en la base y no el propietario de la base misma, que debería responder civilmente ante el primero.

Recordemos aquí que, en realidad, la base de datos es un objeto sobre el cual recae la acción ilícita pero no se trata en realidad del objeto jurídicamente protegido por el ordenamiento (privacidad), como se ha señalado en la doctrina. A partir de allí, y al no existir autorización legal expresa en el Anteproyecto, se podría discutir con total razón la falta de legitimidad de dicho sujeto (propietario de la base) para iniciar la persecución penal contra el sujeto activo.

3 | Síntesis

Nos hemos dedicado aquí al análisis único y exclusivo de la Parte General del Código Penal y del Anteproyecto en el entendimiento de que allí era donde se encontraban las mayores críticas que podían formularse a la situación de los **delitos informáticos** en la legislación actualmente vigente y, además, por considerar que las figuras específicas no presentaban defectos serios en su formulación que las hagan globalmente incongruentes con las restantes normas penales y civiles. Además, adelantamos que parte de las redacciones de las figuras penales de la Parte Especial han sido mejoradas, pero su análisis merece trabajo específico y separado, distinto del que se plantea en estas breves referencias.

En cuanto a lo producido en el Anteproyecto para la Parte General y su comparación con la actual redacción, con referencia la cuestión especial que nos ocupa, solo podemos afirmar una parcial conformidad anclada únicamente en la solución dada a los problemas del ejercicio de la acción penal que, lamentablemente, tampoco ha sido lo suficientemente completa y abarcativa respecto de la legitimidad relacionada con los bancos de datos personales. A su vez, optamos por no pronunciar una advertencia negativa en cuanto a la ausencia de protección penal para la firma electrónica, pues si bien dicho sistema puede ser objeto de las mismas acciones ilícitas de la denominada firma digital, resulta en definitiva una compartida decisión de política criminal destinada a no ampliar el sistema punitivo.

Finalmente, sí debemos remarcar la errada omisión relativa al problema de la falsificación de instrumentos públicos digitales, sobre lo que, debemos reconocer, a lo largo de charlas y debates producidos en foros, paneles y clases relativas al tema, y con juristas que participaron en la elaboración de la ley 26.388, nunca se justificó de manera contundente la actual redacción del Código Penal y sus posibles consecuencias de atipicidad para la falsificación de una orden de allanamiento digital.

No obstante, el Anteproyecto bajo análisis seguirá siendo sometido a debate y discusión, con amplias probabilidades de ser receptor de modificaciones parciales a su estructura; por ello, el significado de estas páginas cobran importancia en cuanto a los objetivos finales planteados, que no son otros que los de colaborar en la elaboración de un sistema penal coherente y eficiente que garantice un mejor servicio en la administración de justicia.

La criminalidad informática en el Anteproyecto de Código Penal de la Nación

por **CARLOS CHRISTIAN SUEIRO**[1]

I | Introducción

El siguiente trabajo tiene por finalidad realizar un análisis de la legislación nacional en materia de criminalidad informática, adentrándose en el estudio del reciente Anteproyecto de Ley de Reforma, Actualización e Integración del Código Penal de la Nación (decreto 678/2012), a efectos de poder establecer qué reformas y actualizaciones resultan indispensables para lograr una política criminal eficiente en torno al tratamiento de los delitos de alta tecnología o perpetrados mediante dispositivos digitales.

Para poder abordar esta temática, dividiremos el trabajo en cuatro etapas o ejes analíticos.

El primero de ellos denominado "La sociedad del siglo XXI, la sociedad de la información", tendrá por finalidad exhibir cómo las tecnologías de la informática y de la comunicación han modificado todas nuestras actividades culturales tales como la política, la economía, la sociología, la medicina, la biónica, la genética, el derecho, las relaciones exteriores, las comunicaciones, la educación, la pedagogía, los servicios de transporte, la música o el arte.

(1) Abogado, especialista en Derecho Penal (UBA). Realizó estudios en Göttingen, Alemania (2011), Salzburg, Austria (2012) y Siracusa, Italia (2013). Jefe de Trabajos Prácticos de las cátedras de los Dres. Alagia y Niño (UBA). Secretario Letrado de la Defensoría Oficial ante la CSJN.

El segundo punto centrará su análisis en los "Antecedentes nacionales y las leyes de reforma en materia de criminalidad informática al Código Penal de la Nación (leyes 26.388, 26.685 y 26.904)", a los fines de conocer con qué dispositivos normativos se cuenta en la actualidad en nuestro país para afrontar la criminalidad de alta tecnología.

Luego de abordar nuestras disposiciones legales vigentes en materia de criminalidad informática, daremos paso, en un tercer apartado, al estudio y análisis de "La criminalidad informática en el Anteproyecto de Ley de Reforma, Actualización e Integración al Código Penal de la Nación (decreto 678/2012)", a fin de conocer qué actualizaciones y reformas se han propuesto en materia de delitos cometidos a través de medios informáticos o dispositivos digitales.

En una cuarta y última etapa, realizaremos nuestras "Recomendaciones y sugerencias en torno a la actualización de la ley penal y procesal penal en materia de criminalidad informática", conforme el estado actual de la legislación nacional y la infraestructura disponible por la administración de justicia a los efectos de poder afrontar este cambio paradigmático, que implica el traspaso de una sociedad analógica propia de finales del siglo XX a una sociedad digital propia del siglo XXI.

Finalmente, se presentan las conclusiones.

2 | La sociedad del siglo XXI, la sociedad de la información

Sin lugar a dudas, la sociedad del siglo XXI se encuentra definida y caracterizada por el avance de las tecnologías de la información y comunicación (TIC), y cómo ellas han modificado cada una de las actividades culturales que la comunidad realiza y despliega diariamente, influyendo así en la política, la economía, la sociología, la medicina, la biónica, la genética, el derecho, las relaciones exteriores, las comunicaciones, la educación, la pedagogía o los servicios de transporte, entre muchas otras.

En virtud del impacto e influencia que la informática ha tenido en la sociedad de fines del siglo XX y de la primera década del siglo XXI es que a la sociedad actual se la conoce o define como la "sociedad de la información".

Sería inimaginable en nuestros días pensar una sociedad sin Internet ni el empleo de motores de búsqueda tales como *Google*[2] o *Yahoo* ni el uso de correos electrónicos (*e-mails*), mensajes de texto (*sms*), mensajería instantánea (*mms*), micromensajería (*Twitter*), chats (*Messenger, Messenger Yahoo, BlackBerry Messenger, Google Talk, Whatsapp, Line, Viber*), blogs, fotologs, redes sociales (*Facebook*,[3] *MySpace, Sonico, Hi5, Orkut, Haboo Hotel, LinkedIn*), o programas de geolocalización como *Foursquare*.

Es más, estos medios de comunicación electrónicos a los cuales acudimos diariamente, hoy no solo se encuentran disponibles en computadoras de escritorio o portátiles como *notebooks, netbooks, ultrabooks* o *tablets*, sino también en teléfonos celulares inteligentes (*smartphones*) y más recientemente hasta en relojes inteligentes (*SmartWatch*)[4] y anteojos inteligentes (*Google Glass Proyect*). Tan indispensables se nos han convertido estas nuevas tecnologías de la informática y la comunicación en todas nuestras labores cotidianas que incluso han generado que a raíz de su empleo constante y habitual haya surgido la necesidad de trasladar las reglas de cortesía básica a las comunicaciones realizadas a través de dispositivos electrónicos debido a la habitualidad de su empleo y al desplazamiento y desuso de los medios tradicionales de comunicación, como por ejemplo, el correo postal.

Por ello,

> "con el avance de la tecnología, las reglas de cortesía, que constituían las normas básicas de la conversación o la correspondencia, se han trasladado desde el lenguaje oral y el género epistolar a la red, a tal punto que, según los expertos, todo navegante educado deberá observar un buen número de normas de *netiqueta*; este neologismo es una castellanización del inglés *netiquette*".[5]

(2) Sobre la evolución de *Google* como motor de búsqueda ver Reischl, Gerald, *El engaño Google. Una potencia mundial sin control en Internet*, (trads. Héctor Piquer y Cristina Sánchez), 1ª ed., Bs. As., Sudamericana, 2009; y Cassin, Barbara, *Googléame. La segunda misión de los Estados Unidos,* 1ª ed., Bs. As., FCE, 2008.

(3) Sobre la irrupción de Facebook ver Faerman, Juan, *Faceboom. El nuevo fenómeno de masas Facebook*, Bs. As., Ediciones B, 2009.

(4) Es el caso de los recientes modelos lanzados por las firmas *Sony (SmartWatch), Apple (iPhone Wrist & iWatch), Samsung (Samsumg Galaxy Gear) y Motorola (Moto Actv).*

(5) De Gavaldá y Castro, Rubén A., *Ceremonial. Un arte para comprender la vida*, Bs. As., Paidós, 2010, p. 85.

El surgimiento de reglas de cortesía mínima o normas básicas de conversación en el ambiente digital no constituye una cuestión menor, sino que todo lo contrario; como refiere el filólogo e historiador francés Milad Doueihi, el desarrollo de la informática y las tecnologías de la comunicación han influido tan profundamente en estas últimas décadas en nuestro desarrollo como civilización que una prueba cabal de ello lo constituye sin lugar a dudas el advenimiento de la *netiqueta*.(6)

Es más, tal ha sido el impacto de la informática a nivel sociológico que no solo ha llevado al advenimiento de la *netiqueta*, sino que ha generado también el surgimiento de grupos de identidad basados tanto en el contacto social directo como a través de sitios virtuales como blogs, fotologs o redes sociales, como es el caso de denominados los *floggers*.

Pero el irrefrenable avance de las telecomunicaciones y la informática ha generado cambios sociales más radicales que el nacimiento de la *netiqueta* o el surgimiento de grupos de identidad virtual como los *floggers*, pues también ha dado lugar, incluso, a distinguir generaciones en períodos más breves de tiempo y en relación directa a la edad del sujeto con la evolución de la informática y las tecnologías digitales al momento de desarrollo de su adolescencia o inicios de su vida adulta.

Es así como en la actualidad se habla de la convivencia de tres generaciones: una "X",(7) otra "Y"(8) y una más, la "Z".(9) Este inusitado avance de la tecnología y el impacto que ella ha generado en la sociedad en pocos

(6) Doueihi, Milad, *La gran conversión digital*, (trad. Julia Bucci), Bs. As., FCE, 2010, p. 21.

(7) La generación "X" está integrada por personas nacidas entre finales de los años 60 y la década de los 70, más precisamente entre 1970 y 1981, y que es la generación que desarrolló su adolescencia entre los años 80 y 90, viviendo los primeros pasos e inicios de la era digital y adaptándose a ella.

(8) La generación "Y" está constituida por personas nacidas entre 1982 y 1992, que desarrollaron su adolescencia en la década de los 90 y la primera década del siglo XXI, teniendo una gran familiaridad con los desarrollos tecnológicos tales como las *PC*, *notebook*, *CD*, *CDROM*, video juegos, radios digitales, y los primeros celulares.

(9) La generación "Z", que está comprendida por las personas nacidas entre 1993 y 2004, que viven actualmente su adolescencia, son quienes no han conocido una sociedad sin computadoras de escritorio, *notebook*, *netbook*, teléfonos celulares, *Internet*, correos electrónicos (*e-mails*), mensajes de texto (*sms*), mensajería instantánea (*mms*), micromensajería (*Twitter*), motores de búsqueda como *Google* o *Yahoo*, redes sociales (*Facebook*, *Myspace*, *Sonico*, *Hi5*, *Orkut*, o *Habbo Hotel*), blogs, fotologs, etc.

años es lo que llevó a que en 2001 Marc Prensky acuñara el término **nativos digitales**

> "para definir a quienes nacieron en un mundo constituido por y alrededor de tecnologías digitales, una tecnología diferente y distante de las que enmarcaron la vida de los adultos de la generación anterior. Para Prensky, esta circunstancia ha generado una brecha entre una y otra generación, los 'nativos' (que nacieron en su entorno) y los 'inmigrantes', adultos para quienes esta tecnología les adviene en sus vidas".(10)

Como puede apreciarse, las tecnologías de la informática y las comunicaciones han impactado contundentemente en nuestro desarrollo como sociedad. Sin embargo, el impacto de estas nuevas tecnologías se extienden incluso más allá, pues han generado grandes cambios a nivel sociológico, filológico, comunicacional, generacional, y también han abarcado otras áreas tales como la medicina, la biónica, la genética, la neurológica, la pedagogía, entre tantas otras. Para el neurocientífico Gary Small y su colaboradora Gigi Vorgan:

> "la actual eclosión de la tecnología digital no solo está cambiando nuestra forma de vivir y comunicarnos, sino que está alterando, rápida y profundamente, nuestro cerebro,(11) (...) seamos nativos o inmigrantes digitales, la alteración de nuestras redes neuronales y conexiones sinápticas mediante actividades como el correo electrónico, los videojuegos, (...) u otras experiencias tecnológicas agudizan, sin duda, ciertas habilidades cognitivas. Podemos aprender a reaccionar más deprisa a los estímulos visuales, y mejorar muchas formas de atención, en particular la capacidad de observar las imágenes de nuestra visión periférica. Desarrollamos una mejor destreza para tamizar rápidamente gran cantidad de información y decidir qué es importante y qué no lo es...".(12)

(10) Balardini, Sergio, "Hacia un entendimiento de la interacción de los adolescentes con los dispositivos de la Web 2.0. El caso de Facebook", en Barindelli y Gregorio (comps.), *Datos personales y libertad de expresión en las redes sociales digitales. Memorándum de Montevideo*, Bs. As., Ad-Hoc, 2010, p. 85.

(11) Small, Gary y Vorgan, Gigi, *El cerebro digital. Cómo las nuevas tecnologías están cambiando nuestra mente*", (trad. Roc Filella Escolá), Barcelona, Urano, 2009, p. 15.

(12) Small y Vorgan, *ibid*., p. 36.

En definitiva, "la tecnología digital, además de influir en como pensamos, nos está cambiando la forma de sentir y comportarnos, y el modo de funcionar de nuestro cerebro".(13)

Tal es así que estas nuevas tecnologías nos están dotando, como especie, de nuevas capacidades como aprender y reaccionar más deprisa a estímulos visuales y a procesar gran cantidad de información con mayor facilidad.

Sin embargo, también es menester mencionar que han traído nuevas afecciones o enfermedades como consecuencia de la excesiva exposición del usuario, tales como los trastornos de déficit de atención (ADD, *Attention Deficit Disorder*) o el trastorno de déficit de atención con hiperactividad (ADHD, *Attention Déficit Hiperactivity Disorder*).(14)

Además de los datos y estudios que la neurociencia nos reporta que las tecnologías digitales están efectuando en nuestro aparato psíquico, la evolución de la informática y de las TIC ha comenzado a generar grandes cambios en otras áreas del desarrollo humano.

En medicina, la informática y las nuevas tecnologías digitales han influido fuerte y significativamente, en un primer momento a través de la digitalización e informatización del instrumental médico.

Así es como en la actualidad "la empresa 3M vende estetoscopios que digitalizan los sonidos..." y "los cardiodesfibriladores son ahora minúsculos chips que se implantan en el pecho de los pacientes y van 'dictando' vía internet cada dato que recogen".(15)

No obstante, las nuevas tecnologías de la información y comunicación no solo han permitido la digitalización del instrumental médico, sino que han otorgado un nuevo horizonte a la biónica.

La biónica, como rama de la medicina dedicada a la integración de circuitos electrónicos en el cuerpo humano a modo de prótesis e implantes

(13) *Ibid.*, p. 16.

(14) *Ibid.*, pp. 84/85.

(15) Ivoskus, Daniel, *Obsesión digital. Usos y abusos en la red,* Bs. As., Norma, 2010, p. 19.

conectados al organismo para restaurar funciones damnificadas, genera grandes expectativas en la actualidad debido al acelerado avance de la informática y en particular a la miniaturización de los componentes electrónicos biocompatibles.

En la actualidad "existe un software que permite mover el cursor de una pantalla solo con el movimiento de la cabeza o de los ojos, depositarlo sobre una letra y transformar lo que 'lee' en frases con sonido. Este sistema permite a un usuario imposibilitado físicamente navegar por internet, abrir su casilla de *email* y mandar SMS a celulares".(16)

Aún más sorprendentes son los desarrollos efectuados en investigación por la compañía Cyberkinectics, la cual "ya está efectuando pruebas clínicas de un implante cerebral que permite a pacientes paralíticos el uso de computadoras mediante controles puramente mentales". De esta manera, "un paciente inmovilizado del cuello para abajo pudo manejar objetos a distancia gracias a un microchip instalado en su cerebro...".(17)

Pero además de los avances en medicina y biónica como consecuencia del impacto de la informática y las nuevas tecnologías digitales, más sorprendente resulta la fusión de avances con otras áreas. La informática, teleinformática, telecomunicaciones, genética, biónica, biotecnología, nanomedicina, han dado lugar a que en la actualidad se haya comenzado a investigar la transmisión de información entre organismos vivos y circuito electrónicos.

Esto que parece digno del guión de una película de ciencia ficción o producto de una mente muy imaginativa o creativa resulta factible hoy en día.

Es así como en el presente ha llegado a sugerirse la bioprogramación como mecanismo válido de superación de la pedagogía tradicional como medio de obtención de información. El autor Ray Kurzweil sostiene que

> "el cerebro dejará de tener un límite establecido por la naturaleza (...) Más allá de los implantes de memoria artificial, el cien-

(16) Ivoskus, *ibid.*, p. 19.

(17) Sibilia, Paula, *El hombre postorgánico. Cuerpo, subjetividad y tecnologías digitales*, 2ª ed., Bs. As., FCE, 2009, p. 128.

> tífico destaca la posibilidad de introducir datos en el cerebro a través de canales neurales directos. Por lo tanto, sería posible aumentar la capacidad de almacenar información a velocidades inusitadas, dejando obsoletos los arduos métodos de aprendizaje tradicionales".(18)

Como puede apreciarse en este primer apartado, tal ha sido el impacto e influencia de la informática y las tecnologías digitales de la comunicación: la *netiqueta*, el advenimiento de grupos de identidad basados en sitios blogs o fotologs (*floggers)*, la distinción de generaciones en períodos de tiempo más breves y acotados ("nativos digitales" o "inmigrantes digitales" o generaciones "X", "Y" o "Z"), la adquisición de nuevas capacidades cognitivas como consecuencia de la exposición a estas nuevas tecnologías y el surgimiento de afecciones tales como trastornos de déficit de atención a raíz de una excesiva exposición a ellas.

También constituyen prueba cabal de su profunda influencia la digitalización del instrumental médico, los avances en biónica mediante la introducción de implantes o prótesis con circuitos electrónicos biocompatibles destinados a restaurar funciones damnificadas o el empleo de la bioprogramación para la transmisión directa de información al cerebro humano a través de la compatibilidad o integración de organismos biológicos con organismos cibernéticos.

Frente a una sociedad cada vez más dependiente de la informática y las tecnologías digitales de la comunicación, la comunidad jurídica argentina se cuestionó hace más de dos décadas el dictado y sanción de una ley que previera la posible comisión de conductas típicas a través del empleo de medios informáticos o dispositivos electrónicos, como así también la protección jurídica de bienes intangibles.

Fue así como hace solo cinco años se produjo la sanción de la ley 26.388 de reforma en materia de criminalidad informática al Código Penal de la Nación, a lo cual se le sumaría la promulgación de las leyes 26.685 y 26.904.

(18) Sibilia, Paula, *ibid.*, p. 123.

3 | Antecedentes nacionales y leyes de reforma en materia de criminalidad informática al Código Penal de la Nación (leyes 26.388, 26.685 y 26.904)

La comunidad jurídica argentina se interrogó tempranamente por el dictado y sanción de una ley que previera la protección de bienes intangibles y la posible comisión de conductas típicas a través del empleo de medios informáticos o tecnologías digitales.

Fue así como desde el año 1996 hasta el año 2008 se presentaron numerosos proyectos de ley destinados a reformar el Código Penal de la Nación mediante una ley integral y concordada para adaptar cada tipo penal a esta nueva modalidad comisiva o bien a través de la sanción de una ley complementaria con idénticas finalidades.

Así podemos mencionar como proyectos de ley presentados durante el período 1996-2008 los siguientes:

1. Proyecto de Ley de Leonor Esther Tolomeo de 1996;
2. Proyecto de Ley de Carlos "Chacho" Álvarez (1996);
3. Proyecto de Ley José A. Romero Feris (1996);
4. Proyecto de Ley de Antonio Tomás Berhongaray (1997);
5. Proyecto de Ley de Anteproyecto de Ley de 2001;
6. Proyecto de Ley Marta Osorio (1225-D-05);
7. Proyecto de Ley de Silvia Virginia Martínez (1798-D-05);
8. Proyecto de Ley Andrés L. Sotos (985-D-05);
9. Delia Beatriz Bisutti (2032-D-06);
10. Dante Omar Canevarolo (3001-D-06);
11. Diana Conti y Agustín Rossi (2291-D-06);
12. Proyecto de Ley de Reforma y Actualización Integral del Código Penal de la Nación (resoluciones MJyDH 303/2004 y 136/2005) hasta culminar en el Proyecto de Ley (CD-109/06; S-1751-1875 y 4417/06 y expediente 5864-D-2006) que dio origen a la presente ley 26.388.

Este último surgió del tratamiento de un gran número de expedientes legislativos y se presenta como una versión por demás mejorada y refinada de todos los anteriores proyectos de ley desde 1996 hasta 2008.

Finalmente, la ley 26.388 fue sancionada el 04/06/2008, promulgada el 24/06/2008 y publicada en el Boletín Oficial de la República Argentina el 25/06/2008.

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 venía debatiendo durante más de dos décadas (1996-2008) y que se hacían presentes en cada uno de los proyectos de ley antes enunciados.

Es así como la ley 26.388 ha alcanzado con su reforma un número muy limitado y específico de tipos penales como lo son:

1. El ofrecimiento y distribución de imágenes relacionadas con pornografía infantil (art. 128 CP),
2. Violación de correspondencia electrónica (art. 153 CP),
3. Acceso ilegítimo a un sistema informático (art. 153 *bis* CP),
4. Publicación abusiva de correspondencia (art. 155 CP),
5. Revelación de secretos (art. 157 CP),
6. Delitos relacionados con la protección de datos personales (art. 157 *bis* CP),
7. Defraudación informática (art. 173, inc. 16 CP),
8. Daño (arts. 183 y 184 CP),
9. Interrupción o entorpecimiento de las comunicaciones (art. 197 CP),
10. El tipo penal de alteración, sustracción, ocultación, destrucción e inutilización de medios de prueba (art. 255 CP), a lo cual debe agregarse las modificaciones terminológicas realizadas en el art. 77 CP.

Es así como contamos con una reforma que ha llevado doce (12) años de elaboración y que ha tomado como sustento otros trece (13) proyectos legislativos, modificando y adaptando tipos penales tradicionales para que puedan ser perpetrados o realizados a través de medios informáticos o dispositivos electrónicos.

Asimismo, debe destacarse que el dictado de la ley 26.388 de reforma al Código Penal de la Nación en materia de criminalidad informática cobra mayor significado y relevancia tras la sanción en el año 2011 de la ley que buscaba la despapelización y la digitalización de la Administración de Justicia; nos referimos más precisamente a la ley 26.685.

El jueves 7 de julio de 2011 se publicó la ley 26.685[19] que otorga a los "expedientes electrónicos, documentos electrónicos, firmas digitales y electrónicas, comunicaciones electrónicas, y domicilios constituidos [la misma] eficacia jurídica y valor probatorio" que en el soporte papel.

Como bien alude Horacio R. Granero, la ley 26.685 es producto del "Plan Estratégico de Modernización de la Justicia que ha encarado la Corte Suprema de Justicia de la Nación que es, sin dudas, una proyección ambiciosa, pero a la vez realista, encaminada a transformar en los próximos años el servicio público de Justicia".[20]

La ley 26.685 que introduce el domicilio electrónico y el expediente digital cuenta con dos (2) artículos de fondo y uno de forma.

El art. 1 de la ley 26.685 dispone: "Autorízase la utilización de expedientes electrónicos, documentos electrónicos, firmas electrónicas, firmas digitales, comunicaciones electrónicas y domicilios electrónicos constituidos, en todos los procesos judiciales y administrativos que se tramitan ante el Poder Judicial de la Nación, con idéntica eficacia jurídica y valor probatorio que sus equivalentes convencionales".

Mientras que el art. 2 establece que "La Corte Suprema de Justicia de la Nación y el Consejo de la Magistratura de la Nación, de manera conjunta, reglamentarán su utilización y dispondrán su gradual implementación".

Es así como la Corte Suprema de Justicia de la Nación desde la sanción de la ley 26.685, ha profundizado sus esfuerzos a fin de materializar la aplicación del expediente digital y que este no se transforme en una mera declaración de buenas intenciones por parte de la ley.

(19) BO, 07/07/2011.

(20) Granero, Horacio R., "La sanción de la Ley 26.685 de Expedientes Digitales. El principio de equivalencia funcional y la firma digital", [en línea] *elDial.com*, CC2736.

Pueden destacarse como actos tendientes por parte de la Corte Suprema de Justicia de la Nación, orientados a la concreción y materialización del empleo del expediente digital:

1. La creación de la "Biblioteca Jurídica Digital de la CSJN, Dr. Rodolfo G. Valenzuela" el 31/10/2011.(21)

2. La reglamentación, desde el 13/12/2011, del "Sistema de Notificación Electrónica (SNE)".(22)

3. La puesta en funcionamiento del "Sistema de Notificación Electrónica (SNE)", de aplicación obligatoria desde el 07/05/2012, para la interposición de recursos de queja por denegación de recurso extraordinario federal.(23)

4. El establecimiento a partir del 01/06/2012 del "Libro de Asistencia de Letrados (Libro de Notas) dentro del programa informático" de seguimiento de causas de la CSJN, que actualmente se realiza de en soporte papel.(24)

5. La extensión de la aplicación obligatoria del Sistema de Notificación Electrónica a todos los fueros y en diversas materias.(25)

La Corte Suprema de Justicia de la Nación no ha sido la única que ha dado grandes avances en materia de digitalización del servicio brindado por la administración de justicia, como bien menciona Gisela Candarle, "la Justicia de la Ciudad de Buenos Aires ha dado pasos significativos en la formulación de sistemas de gestión bajo soporte digital".(26)

(21) CSJN, Acordada 28/2011, [en línea] www.csjn.gov.ar

(22) CSJN, Acordada 31/2011, [en línea] www.csjn.gov.ar.

(23) CSJN, Acordada 3/2012, [en línea] www.csjn.gov.ar.

(24) CSJN, Acordada 8/2012, [en línea] www.csjn.gov.ar.

(25) CSJN, Acordada 29/2012, "Aplicación obligatoria del Sistema de Notificación Electrónica para los Tribunales Provinciales en los que se tramite un Recurso Extraordinario Federal o un Recurso de Queja por Extraordinario denegado". CSJN, Acordada 14/2013, "Se dispone la aplicación obligatoria del Sistema Informático de Gestión Judicial (SGJ) para todos los fueros". CSJN, Acordada 35/2013, "Ampliación del Sistema de Notificación Electrónica a las presentaciones por retardo de justicia y presentaciones varias ante la CSJN". CSJN, Acordada 36/2013, "Ampliación del Sistema de Notificación Electrónica a las presentaciones efectuadas en causas originarias ante la CSJN". CSJN, Acordada 38/2013, "Ampliación del Sistema de Notificación Electrónica a todos los fueros, implementándose a través de las Cámaras Nacionales y Federales". CSJN, Acordada 43/2013, "Ampliación del SNE a todos los Superiores Tribunales de Provincia y a la Ciudad Autónoma de Buenos Aires", [en línea] www.csjn.gov.ar.

(26) Candarle, Gisela, "Hacia la justicia digital en la Ciudad de Buenos Aires", [en línea] *elDial.com*, DC167D.

Además de la sanción de la ley 26.388 de reforma al Código Penal de la Nación en materia de criminalidad informática y de la ley 26.685 de implementación del expediente digital y la notificación electrónica, en el último año se ha realizado una reforma específica y puntual que amplía el catálogo de delitos por medio de la ley 26.904.

Le ley 26.904[27] introduce la figura del *grooming* al Código Penal de la Nación a través de la nueva redacción del art. 131, el cual establece que "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".

Como refiere Hugo Vaninetti, el *grooming* "engloba básicamente la realización de actos preparatorios a través de las modernas tecnologías de la comunicación e información para perpetrar posteriormente delitos contra la integridad sexual. Importaría decir que es una etapa virtual previa al abuso sexual en el mundo real".[28]

Con esta última ley 26.904 tenemos una visión panorámica del marco de la legislativo de la República Argentina en materia de criminalidad informática, conformada así por la ley 26.388 de reforma en materia de criminalidad informática al Código Penal de la Nación, la ley 26.685 de implementación del expediente digital y la notificación electrónica y la reciente ley 26.904 que incorpora la figura del *grooming* al catálogo de delitos ya preestablecido por la ley 26.388 al Código Penal de la Nación.

Habiendo dejado en claro las disposiciones legales vigentes en materia de criminalidad informática en el sistema legislativo nacional procederemos a verificar qué reformas propone el Anteproyecto de Ley de Reforma, Actualización e Integración al Código Penal de la Nación.

(27) BO 11/12/2013.

(28) Vaninetti, Hugo A., "Inclusión del '*grooming*' en el Código Penal", Bs. As., La Ley, 2013, AR/DOC/4628/2013. También sobre *grooming* se sugiere ver Vaninetti, Hugo A., "Media sanción del Senado al proyecto de '*grooming*'", publicado en el Suplemento de Actualidad de la Ley, Bs. As., 26/04/2012. Lo Giudice, María Eugenia, "Con motivo de la sanción de la ley que introduce el 'delito de *grooming*' en el Código Penal (año 2013)", en *elDial.com*, DC1C0B.

4 | La criminalidad informática en el Anteproyecto de Código Penal de la Nación

Desde inicios de la primera década de este siglo XXI, la República Argentina se ha propuesto la recodificación de su legislación penal, buscando la supresión de las leyes complementarias y llevando a cabo un proceso de reforma y actualización integral del Código Penal de la Nación.

Una prueba cabal de ello fue el Anteproyecto de Ley de Reforma y Actualización integral del Código Penal de la Nación de 2006 (MJyDH, resoluciones 303/2004 y 136/2005),[29] elaborado por una Comisión de los más destacados juristas nacionales que había sido convocada por el Ministerio de Justicia y Derechos Humanos bajo la coordinación de la Secretaría de Política Criminal y Asuntos Penitenciarios. Anteproyecto este que no resultó tratado en el Honorable Congreso de la Nación por razones de índole netamente política.

No obstante, a partir del año 2012 fue puesto en marcha un nuevo proceso de recodificación de la legislación penal por medio de la creación de una Comisión para la Elaboración del Anteproyecto de Ley de Reforma, Actualización e Integración del Código Penal de la Nación,[30] conformada por el Sr. Profesor Emérito de la Universidad de Buenos Aires, Dr. Eugenio Raúl Zaffaroni, los diputados Ricardo Gil Lavedra de Unión Cívica Radical y Federico Pinedo de la Alianza Propuesta Republicana y los abogados María Elena Barbagelata del Partido Socialista/Frente de Acción Progresista y León Carlos Arslanián por el Partido Justicialista, lo que exhibe la pluralidad partidaria al momento de conformar la comisión elaboradora y redactora del Proyecto.

Como bien nos expresa el Sr. Profesor Dr. Daniel Pastor,

> "la reforma iniciada tiene la finalidad explícita de integrar en un solo cuerpo normativo toda la legislación penal hoy disper-

(29) Ver Anteproyecto de Ley de Reforma y Actualización Integral del Código Penal de la Nación (MJyDH, resoluciones 303/2004 y 136/2005).

(30) Decreto 678/2012, BO 08/05/2012.

> sa y desarmonizada por una descodificación que ha alterado el equilibrio y la proporcionalidad que deben tener las disposiciones represivas, con lo cual se ha afectado la sistematicidad normativa, aspecto de la legislación penal que no es un adorno intelectual, sino garantía de efectividad de los principios de legalidad y culpabilidad (seguridad y previsibilidad), que son el corazón del derecho penal liberal".(31)

Es así como el jueves 13 de febrero de 2014 la Comisión encargada de la elaboración del Anteproyecto de Reforma presentó al Poder Ejecutivo de la Nación el Anteproyecto de Ley de Reforma, Actualización e Integración del Código Penal de la Nación.

A continuación, analizaremos desde la óptica de la criminalidad informática el Anteproyecto de Ley de Reforma, Actualización e Integración del Código Penal de la Nación, a los fines de relevar y dilucidar qué reformas y actualizaciones propone para los delitos perpetrados mediante el empleo de las nuevas tecnologías y dispositivos digitales.

4.1 | Parte general. Terminología y definiciones

El actual Código Penal de la Nación, tras la reforma de la ley 26.388, estableció en el art. 77 la conceptualización de los términos "documento", "firma", "suscripción" e "instrumento privado".

Es así como el art. 77 CP reza:

> "... El término 'documento' comprende toda representación de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión.
>
> Los términos 'firma' y 'suscripción' comprenden la firma digital, la creación de una firma digital o firmar digitalmente.
>
> Los términos 'instrumento privado' y 'certificado' comprenden el documento digital firmado digitalmente...".

(31) Pastor, Daniel, "La recodificación penal en marcha. Una iniciativa ideal para la racionalización legislativa", en *Pensar en Derecho*, Bs. As., Eudeba/Facultad de Derecho (UBA), 2012, p. 38.

El Anteproyecto de Ley de Reforma, Actualización e Integración del Código Penal de la Nación, en la Parte General, ha dedicado dentro del Título XIV destinado a la "Significación de conceptos empleados en el Código", un artículo más, específicamente el art. 69, para otorgar las definiciones de: "reglamento", "ordenanzas", "funcionario público", "mercadería", "capitán", "tripulación", "estupefaciente", "establecimiento rural", "violencia", y así también la definición de "firma digital", "documento", etc.

Es así que en en el primer borrador de trabajo, el art. 69 del Proyecto de Ley de Reforma, Actualización e Integración del Código Penal de la Nación, disponía en lo referente a los términos "documento", "firma", "suscripción" e "instrumento privado", lo siguiente:

> "k) Los términos 'firma' y 'suscripción' comprenden la firma digital, la creación de una firma digital o firmar digitalmente. Los términos 'documento', 'instrumento privado' y 'certificado' comprenden al documento digital firmado digitalmente".
>
> l) Se considerará 'documento' a la representación de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento o archivo que contenga datos".

Como puede apreciarse a simple vista, la Comisión Redactora del Anteproyecto de Ley de Reforma, Actualización e Integración del Código Penal de la Nación había decidido conservar, pese al orden otorgado, la redacción original de la ley 26.388.

No obstante, en su versión final y definitiva del Anteproyecto del Proyecto de Ley de Reforma, Actualización e Integración del Código Penal de la Nación se dispone la teminología y conceptualización en el art. 63, incs. s) y t), el cual dispone:

> "s) Por 'sistema informático' se entiende todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa.
>
> t) 'Dato informático' es toda representación de hechos, información o conceptos expresados de cualquier forma, que se preste a tratamiento informático, incluidos los programas diseñados para

> que un sistema informático ejecute una función. El término comprende, además, los datos relativos al tráfico, entendiendo como tales todos los relativos a una comunicación realizada por medio de un sistema informático, generados por este último en tanto que elemento de la cadena de comunicación, y que indican el origen, el destino, la ruta, la hora, la fecha, el tamaño y la duración de la comunicación o el tipo de servicio subyacente".

Se presenta una versión mejorada respecto a la actual redacción del Código Penal de la Nación y al primer borrador de trabajo utilizado por la Comisión, en relación a la conceptualización y teminología, esta nueva redacción y técnica legislativa resulta ser mucho más adecuada, actualizada y versátil a la dinámica de la materia de la criminalidad informática.

4.2 | Parte especial. El tipo penal de ofrecimiento y distribución de imágenes relacionadas con pornografía infantil

El tipo penal de ofrecimiento y distribución de imágenes relacionadas con pornografía infantil se encuentra contemplado en el art. 128 CP, el cual dispone que:

> "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 finales 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".

Por su parte, la Comisión de Reforma, Actualización e Integración del Código Penal de la Nación trabajó sobre un borrador para este tipo penal que establecía que:

> "Será reprimido con prisión de seis (6) meses a tres (3) años, el que produjere o publicare imágenes pornográficas en que se exhibieran menores de dieciocho (18) años, al igual que el que organizare espectáculos en vivo con escenas pornográficas en que participaren dichos menores".
>
> En la misma pena incurrirá el que distribuyere imágenes pornográficas cuyas características externas hicieren manifiestas que en ellas se ha grabado o fotografiado la exhibición de menores de dieciocho (18) años de edad al momento de la creación de la imagen".
>
> Será reprimido con prisión de quince (15) días a dos (2) años quien facilitare el acceso a espectáculos pornográficos o suministrare material pornográfico a menores de catorce (14) años".

Como puede apreciarse el primer borrador disminuía el máximo de la pena en un año, pasando de una pena máxima de cuatro (4) años a una máxima de tres (3).

En su redacción puede constatarse que suprimía los ocho verbos típicos empleados por la redacción original ("produjere, financiare, ofreciere, comerciare, publicare, facilitare, divulgare o distribuyere") y los sustituía únicamente por los verbos "producir" y "publicar".

Se mantenía en el segundo párrafo la punición de la tenencia de material pornográfico que exhiba a menores de edad, siempre que sea con fines de distribución, dejando como atípico la mera tenencia de material pornográfico, tal como lo previó la ley 26.388.

En lo pertinente al tercer párrafo, también se mantenía el texto original instaurado por la ley 26.388. En su versión final y definitiva el Anteproyecto optó por la siguiente redacción del tipo penal en su art. 131:

> "1. Será reprimido con prisión de UNO (1) a SEIS (6) años, el que produjere o por cualquier medio publicare, comerciare o

divulgare imágenes de actividades sexuales explícitas de menores.

2. La misma pena se impondrá a quien organizare espectáculos en vivo con escenas pornográficas en que participaren menores.

3. Si los delitos de los incisos precedentes se cometiesen contra menores de trece años, la pena de prisión será de TRES (3) a DIEZ (10) años.

4. El que facilitare el acceso a espectáculos pornográficos o suministrare material pornográfico a menores de trece años, será penado con prisión de UNO (1) a SEIS (6) años."

Como puede apreciarse, en la redacción definitiva realizada por el Anteproyecto respecto a éste tipo penal, se ha mantenido la redacción de la ley 26.388 en gran medida, pero se ha incrementado su escala punitiva.

Su mínimo se ha incrementado en seis (6) meses y su máximo se ha incrementado en dos (2) años, pasando, de seis (6) meses a un (1) año en el caso del mínimo, y para el máximo de los originales cuatro (4) años a seis (6) años de prisión.

Respecto a la facilitación al acceso a espectáculos pornográficos o el suministro de material pornográfico a un menor de trece años, la reforma en su versión final, se ha tornado más represiva.

En primer lugar, ha disminuido la edad del sujeto pasivo de 14 a 13 años, y en segundo orden, ha incrementado la pena en tres (3) años, pasando de un máximo de tres (3) años a un máximo de seis (6) años de prisión.

También ha generado un incremento de la escala original cuando la producción, publicación, comercialización o divulgación de imagines de menores con actividades sexuales explicitas fueran de un menor de 13 años, incrementando la escala hasta un máximo de 10 años.

Claramente resulta más represivo que el tipo penal vigente cuyo máximo era cuatro (4) años de prisión, y ahora se incrementa en seis (6) años la formula agravada, ascendiendo la escala en seis (6) años más de prisión.

4.3 | Los tipos penales de violación de secreto y privacidad

Una de los puntos más relevantes y significativos de la reforma de la ley 26.388 ha sido la ampliación y redefinición del bien jurídico protegido. Dicha ley ha sustituido en el Título V —"Delitos contra la libertad"— el contenido de su Capítulo III de "Violación de Secretos" por "Violación de Secretos y de la Privacidad" en el Libro II del Código Penal de la Nación.

4.3.1. Violación de correspondencia electrónica

Entre los tipos penales que fueron alcanzados por la ley 26.388 encontramos el tipo penal de violación de correspondencia, el cual reza en su 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".

El Proyecto de Ley de Reforma, Actualización e Integración del Código Penal de la Nación preveía en el primer borrador de trabajo respecto a este tipo penal que:

> "Será reprimido con prisión de quince (15) días a seis (6) meses o de diez (10) a doscientos (200) días multa, el que abriere

> indebidamente una carta, un pliego cerrado o un despacho telegráfico, telefónico, mensaje de correo electrónico o de otra naturaleza que no le esté dirigido; o se apoderare indebidamente de una carta, de un pliego, de un mensaje de correo electrónico, de un despacho o de otro papel privado, aunque no esté cerrado; o suprimiere o desviare de su destino una correspondencia o mensaje de correo electrónico que no le esté dirigida.
>
> Se le aplicará prisión de un (1) mes a un (1) año o de diez (10) a trescientos (300) días multa, si el culpable comunicare a otro o publicare el contenido de la carta, escrito, mensaje de correo electrónico o despacho".

En dicho borrador se mantenía, en su primer párrafo, la redacción original del art. 153 CP conforme la ley 26.388. Es así como se consideraban como típicas las conductas de:

1. Apertura o acceso a correspondencia.
2. Apoderamiento de una comunicación electrónica.
3. Supresión y desvío de comunicaciones electrónicas.
4. Interceptación y captación de comunicaciones electrónicas.
5. Comunicación o publicación ilegítima.

No se contempla en esta nueva redacción la agravación de la pena con inhabilitación especial por el doble del tiempo de la pena si la conducta fuera realizada por un funcionario público en la redacción de este artículo.

Por cuestiones de sistematización y ordenamiento concordado del proyecto de reforma, en lugar de incluirlo en el mismo artículo, se lo contemplaba en un artículo por separado que decía que "Cuando en alguno de los artículos de este capítulo hubiese intervenido un funcionario público en desempeño o ejercicio del cargo, se le aplicará además la pena de inhabilitación especial por el doble de tiempo de la condena".

Sin embargo, en su versión final y definitiva, el Anteproyecto de Ley de Reforma, Actualización e Integración del Código Penal de la Nación previó esta figura en el art. 119 con la siguiente redacción:

> "Será reprimido con prisión de SEIS (6) meses a DOS (2) años y multa de DIEZ (10) a CIENTO CINCUENTA (150) días, el que:
>
> a. Abriere o accediere indebidamente una comunicación electrónica, telefónica, una carta, un pliego cerrado, un papel privado, un despacho telegráfico o telefónico o de otra naturaleza, que no le estuviere dirigido.
> b. Se apoderare indebidamente de alguno de ellos, aunque no estuviere cerrado.
> c. Lo suprimiere o desviare de su destino, cuando no le estuviere dirigido.
> d. Interceptare o captare comunicaciones electrónicas o telecomunicaciones provenientes de cualquier sistema de carácter privado o de acceso restringido."

En la redacción final y definitiva del Anteproyecto se mantiene casi textual el texto vigente del art. 153 CP establecido por la ley 26.388.

No obstante debe destacarse el incremento de la escala penal. Respecto al mínimo de la escala pasa de 15 días a seis (6) meses de prisión y en su máximo de seis (6) meses, se eleva a dos (2) años de prisión.

4.3.2. Acceso ilegítimo a un sistema informático

La ley 26.388 contempló la incorporación de la acción de acceso ilegítimo a un sistema informático a través del art. 153 *bis*, el cual reza:

> "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".

El borrador original sobre el que trabajo la Comisión de Reforma disponía, en los arts. 140, 141 y 142, que:

> "Será reprimido con prisión de seis (6) meses a dos (2) años el que, para vulnerar la privacidad de otro, utilice artificios de escucha, transmisión, grabación o reproducción del sonido o ima-

gen" (art. 140, que introducía la figura penal de captaciones de imágenes y sonidos la cual había sido descartada al momento de la sanción de la ley 26.388);

"Se impondrá pena de prisión de seis (6) meses a dos (2) años si se difundieran, revelaran o cedieran a terceros los datos o hechos descubiertos o las imágenes captadas a que se refiere el artículo anterior"(art. 141 del borrador de trabajo, que preveía la difusión o revelación de las imágenes captadas);

"Será reprimido con prisión de seis (6) meses a dos (2) años el que indebidamente interceptare, captare o desviare comunicaciones telefónicas, postales, de telégrafo o facsímil o cualquier otro sistema de envío de objetos o transmisión de imágenes, voces o paquetes de datos, así como cualquier otro tipo de información, archivo, registros y/o documentos privados o de entrada o lectura no autorizada o no accesible al público que no le estuvieren dirigidos.

La pena será de uno (1) a cinco (5) años si el autor fuere funcionario público o integrante de las fuerzas armadas o de seguridad" (Este artículo realizaba una ampliación de las conductas previstas para el acceso ilegítimo a un sistema informático, contemplado también la interceptación, captación y desvío, además del mero acceso ilegítimo a un sistema informático que no sea de índole público).

Sin embargo, en la redacción final y definitiva del Anteproyecto de Ley de Reforma, Actualización e Integración del Código Penal de la Nación, previó contener esta figura en el art. 123 con la siguiente redacción.

"1. Será reprimido con multa de DIEZ (10) a CIEN (100) días, el que a sabiendas accediere por cualquier medio, sin autorización o excediendo la que poseyere, a un sistema o dato informático de acceso restringido.

2. La pena será de SEIS (6) meses a DOS (2) años de prisión cuando el acceso fuere en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos, de salud o financieros. 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.

3. Será penado con prisión de SEIS (6) meses a DOS (2) años el que:

a. A sabiendas y violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales.

b. 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 legal.

c. Insertare o hiciere insertar ilegítimamente datos en un archivo de datos personales.

d. Mediante cualquier ardid o engaño determinare a otro a proveer datos personales, financieros o confidenciales.

e. Tuviere, desarrollare o comerciare artificios técnicos inequívocamente destinados a la indebida obtención de datos personales, financieros o confidenciales.

f. Utilizare la identidad de una persona física o jurídica que no le perteneciere, a través de cualquier medio electrónico, con el propósito de causar perjuicio.

4. Cuando el agente fuere funcionario público sufrirá, además, inhabilitación de UNO (1) a CINCO (5) años."

En la redacción final el Anteproyecto en lugar de mantener la figura de acceso Ilegítimo a un sistema informático en forma disgregada en tres artículos, se decidió unirlos en un único artículo con cuatro puntos.

Asimismo, como modificación se previó que cuando la acción se desplegara "perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos, de salud o financieros", un incremento de la pena que supera la escala original prevista por el art. 153 *bis* CP, pasando de un (1) mes a un (1) año de prisión a seis (6) meses y dos (2) años de prisión.

También es dable destacar que en esta versión final, la escala se incrementa aún más, "Si el hecho se cometiere con el fin de obtener información sensible a la defensa nacional", llegando a elevar el máximo de la pena en cuatro años de prisión.

Por último debe resaltarse que la figura definitiva contemplada en este art. 123, por el Anteproyecto contempla la introducción de una nueva figura punible, en su apartado 3, inciso f, prevé la incorporación de la figura de usurpación de identidad ya sea que se trate, de una persona física o jurídica a través de medios electrónicos.

4.3.3. Publicación abusiva de correspondencia

La ley 26.388 contempló en el art. 155 CP la publicación abusiva de correspondencia con la siguiente redacción:

> "Será reprimido con multa de pesos un mil quinientos ($ 1500) 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".

El borrador sobre el que trabajó originalmente la Comisión de Reforma, Actualización e Integración del Código Penal de la Nación, conservaba esta figura típica tal como podrá apreciarse a continuación:

> "Será reprimido con multa de diez (10) a ciento cincuenta (150) días-multa el que, hallándose en posesión de una correspondencia o mensaje de correo electrónico no destinado a la publicidad, lo hiciere publicar indebidamente, aunque haya sido dirigida a él, si el hecho causare o pudiere causar perjuicios a terceros".

La principal modificación que puede observarse es la sustitución de la pena de multa por días-multa, como así también el reemplazo de la expresión amplia de "comunicación electrónica", establecida por la ley 26.388, por "mensaje de correo electrónico", lo que podría reducir ampliamente la punición de la conducta.

Afirmamos ello toda vez que la expresión comunicación electrónica abarca: correos electrónicos (e-mails) mensajería instantánea (mms), micro-

mensajería (Twitter), *chats* (Messenger, Messenger Yahoo, Google Talk, Whatsapp), *blogs*, fotolog, y redes sociales (Facebook, MySpace, Sonico, Hi5, Orkut, Haboo Hotel, LinkedIn); mientras que la opción de mensajes de correo electrónico resulta mucho más acotada, ya que por conforme el principio de legalidad, es su faz de ley estricta, y quedaría solo acotado a los correos electrónicos, siendo ampliamente debatible si se encuentra incluida la mensajería instantánea, micromensajería, los chats, blogs y redes sociales.

Tampoco contemplaba en esa redacción la exención de responsabilidad penal si la publicación tuviere por objeto proteger el interés público.

Sin embargo en su versión final y definitiva el Anteproyecto de Ley de Reforma, Actualización e Integración del Código Penal de la Nación previó esta figura en el art. 121 con la siguiente redacción.

> "1. Será reprimido con prisión de SEIS (6) meses a TRES (3) años, multa de DIEZ (10) a CIENTO CINCUENTA (150) días e inhabilitación de UNO (1) a CUATRO (4) años el que, hallándose en posesión de un instrumento, registro o contenidos a que se refieren los dos artículos precedentes, lo comunicare, publicare o lo hiciere publicar, indebidamente.
>
> 2. La misma pena se impondrá a quien los hiciere publicar, cuando le hubieren sido dirigidos, siempre que no estuvieren destinados a la publicidad, si el hecho causare o pudiere causar perjuicios.
>
> 3. Estará exento de responsabilidad penal quien hubiere obrado con el propósito inequívoco de proteger un interés público actual".

En su versión final y definitiva la redacción del Anteproyecto mantiene la redacción original del art. 155 CP conforme la ley 26.388, modificando únicamente su escala punitiva, pasando de una pena de multa de la $1500 a 100.000, a un mecanismo de pena conjunta que implica, pena de prisión, multa e inhabilitación, consistiendo de SEIS (6) meses a TRES (3) años, multa de DIEZ (10) a CIENTO CINCUENTA (150) días e inhabilitación de UNO (1) a CUATRO (4) años.

4.3.4. Revelación de secretos

La ley 26.388 previó como otro delito contra la violación de secretos y la privacidad, la violación de secretos, en el art. 157, el cual dispone que:

> "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".

En el primer borrador de trabajo utilizado por la Comisión de Reforma, Actualización e Integración del Código Penal de la Nación, se mantenía la misma redacción modificando únicamente la escala punitiva, como puede chequearse a continuación.

> "Será reprimido con prisión de seis (6) meses a dos (2) años el funcionario público que revelare hechos, actuaciones o documentos que por la ley deben quedar secretos" (art. 145).

No obstante, en su redacción final y definitiva, el Anteproyecto de Ley de Reforma, Actualización e Integración del Código Penal de la Nación, tiene la siguiente descripción típica (art. 122):

> "1. Será reprimido con prisión de SEIS (6) meses a DOS (2) años o multa de DIEZ (10) a CIEN (100) días e inhabilitación por doble tiempo del de la condena, el 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.
>
> 2. La misma pena se impondrá al funcionario público que revelare hechos, datos, actuaciones o documentos que por ley debieren quedar secretos".

La redacción final y definitiva del Anteproyecto de Reforma y Actualización del Código Penal mantuvo en gran medida la redacción original del art. 157 del CP conforme ley 26.388.

La principal variante que se puede apreciar una vez más en la redacción de este tipo penal se vislumbra en su escala pena.

Incrementándose para el caso de la pena de prisión su mínimo en cinco (5) meses, pasando de un (1) mes a seis (6) meses de prisión; imponiéndose una nueva pena como lo es la de multa, que no estaba contemplada en el tipo original y elevándose la pena de inhabiltación por el doble del tiempo de ella condena.

4.3.5. Delitos relacionados con la protección de datos personales

La ley 26.388 procuró también proteger los datos personales contenidos en bases de datos digitalizadas; fue así que se sancionó el art. 157 *bis* CP, el cual dispone que:

> "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 otra 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".

El borrador que sirvió de base al trabajo de la Comisión mantenía la misma redacción modificando únicamente la escala punitiva, incrementando el mínimo de la escala penal de un (1) mes a seis (6) meses de pena de prisión, como puede observarse a continuación.

> "Será reprimido con la pena de prisión de seis (6) meses a dos (2) años el que ilegítimamente accediere, de cualquier forma, a un banco de datos personales.
>
> La misma pena se aplicará al que insertare o hiciere insertar datos falsos en un archivo de datos personales o proporcionare a un tercero información falsa contenida en un archivo de datos personales o revelare a otro información registrada en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de una ley" (art. 146).

En su redacción final y definitiva el Anteproyecto fundió el art. 157 *bis* CP conforme ley 26.388, en el actual tipo penal del art. 123, punto 3, inc. a), b), c), d) y e), fusionando así este tipo penal de "Protección de Datos Personales" (art. 157 *bis*) con el de "Acceso Ilegítimo a un sistema informático" (art.153 *bis*) y con la nueva figura de usurpación de identidad por medios informáticos, y dice:

> "1. Será reprimido con multa de DIEZ (10) a CIEN (100) días, el que a sabiendas accediere por cualquier medio, sin autorización o excediendo la que poseyere, a un sistema o dato informático de acceso restringido.
>
> 2. La pena será de SEIS (6) meses a DOS (2) años de prisión cuando el acceso fuere en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos, de salud o financieros. 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.
>
> 3. Será penado con prisión de SEIS (6) meses a DOS (2) años el que:
>
> a. A sabiendas y violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales.
>
> b. 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 legal.
>
> c. Insertare o hiciere insertar ilegítimamente datos en un archivo de datos personales.
>
> d. Mediante cualquier ardid o engaño determinare a otro a proveer datos personales, financieros o confidenciales.
>
> e. Tuviere, desarrollare o comerciare artificios técnicos inequívocamente destinados a la indebida obtención de datos personales, financieros o confidenciales.
>
> f. Utilizare la identidad de una persona física o jurídica que no le perteneciere, a través de cualquier medio electrónico, con el propósito de causar perjuicio.
>
> 4. Cuando el agente fuere funcionario público sufrirá, además, inhabilitación de UNO (1) a CINCO (5) años."

4.3.6. Violación de privacidad o captación de imágenes y sonidos

Se incorpora un nuevo tipo penal no contemplado por el Código Penal de la Nación, conforme la ley 26.388, que es la violación a la privacidad, este tipo penal había sido tratado al momento de la sanción de la ley 26.388 como el tipo penal de Captación de imágenes y sonido, el cual finalmente en el año 2008 no había sido aprobado y en la actualidad se lo incorpora por vía de esta reforma integral.

> "1. Será reprimido con prisión de SEIS (6) meses a DOS (2) años y multa de DIEZ a CIENTO CINCUENTA días, el que vulnerare la privacidad de otro, mediante la utilización de artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o imagen, o se hiciere de registros no destinados a la publicidad.
>
> 2. El que incurriere en cualquiera de los delitos del presente artículo o del anterior, abusando de su oficio o profesión, o de su condición de funcionario público, será reprimido con prisión de UNO (1) a CUATRO (4) años."

4.4 | El tipo penal de defraudación informática

La ley 26.388 incorporó la por demás cuestionada defraudación informática al Código Penal de la Nación, más precisamente por la redacción que se le otorgó al tipo penal que se trascribe a continuación, en el art. 173, inc. 16, CP:

> "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".

El borrador de trabajo suprimía esta por demás compleja y cuestionada figura de la defraudación informática, dejando subsistente únicamente la figura de la defraudación automatizada prevista en el art. 173, inc. 15 CP.

Finalmente en su versión final y definitiva el Anteproyecto de Ley de Reforma, Actualización e Integración del Código Penal de la Nación, mantuvo la Defraudación Informática con la redacción original de la ley 26.388 en el art. 144, inc. o):

> "El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o de la transmisión de datos".

4.5 | El tipo penal de daño

La reforma de la ley 26.388 introdujo un segundo párrafo al delito de daño, contemplando lo que se conoce como daño a bienes inmateriales o intangibles, el cual dispone en el art. 183, 2° párrafo que:

> "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".

El borrador sobre el que trabajó la Comisión de Reforma mantenía la redacción original de la ley 26.388 y contemplaba el daño a bienes intangibles o inmateriales en el art. 187:

> "Será reprimido con prisión de quince (15) días a un (1) año, el que por cualquier medio, destruya en todo o en parte, borre, altere en forma temporal o permanente, o de cualquier manera impida la utilización de datos o programas contenidos en soportes magnéticos, electrónicos o informáticos de cualquier tipo o durante un proceso de transmisión de datos.
>
> La misma pena se aplicará a quien venda, distribuya, o de cualquier manera haga circular o introduzca en un sistema informático, cualquier programa destinado a causar daños de los prescriptos en el párrafo anterior, en los datos o programas contenidos en una computadora, una base de datos o en cualquier tipo de sistema informático".

Luego de la lectura de ambos artículos puede apreciarse que se seguían empleando los tres verbos típicos "destruir", "alterar" e "inutilizar", aunque agregaba en su nueva redacción el verbo "borrar".

Al igual que la figura original, se penaba en el segundo párrafo la venta, distribución, circulación o introducción de programas destinados a cau-

sar daño, tales como virus o códigos maliciosos; y se mantenía atípica la conducta de diseño o creación de programas destinados a causar daños, virus o códigos maliciosos, siempre y cuando ellos no sean puestos en circulación, distribuidos, vendidos o introducidos en un sistema informático.

Finalmente, la versión definitiva del Anteproyecto de Ley de Reforma, Actualización e Integración del Código Penal de la Nación establece como figura de daño el texto previsto en el art. 161:

> "1. Será reprimido con prisión de SEIS (6) meses a UN (1) año o multa de DIEZ (10) a CIEN (100) días, el que destruyere, inutilizare, hiciere desaparecer o de cualquier modo dañare una cosa mueble o inmueble o un animal, total o parcialmente ajenos.
>
> 2. La misma pena se impondrá al que vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños.
>
> 3. El máximo de la pena de prisión será de CUATRO (4) años cuando el daño:
>
> a. Fuere ejecutado con violencia en las personas, o se emplearen sustancias venenosas o corrosivas.
> b. Fuere ejecutado en cosas de valor científico, artístico, cultural, militar o religioso, o cuando, por el lugar en que se encontraren, se hallaren libradas a la confianza pública o destinadas al servicio o a la utilidad de un número indeterminado de personas.
> c. Recayere sobre medios o vías de comunicación o de tránsito, sobre obras hechas en cursos de agua, o sobre instalaciones destinadas al servicio público.
> d. Se ejecutare en sistemas informáticos destinados a la prestación de servicios de salud, de comunicaciones, de provisión o transporte de energía, u otros servicios públicos.
> e. Se ejecutare en archivos, registros, puentes, caminos u otros bienes de uso público, tumbas, signos o símbolos conmemorativos.
> f. Produjere infecciones o contagios en aves o en otros animales domésticos o ganado.
> g. Se cometiere sobre yacimientos arqueológicos o paleontológicos, sobre bienes provenientes de éstos, o sobre cualquier otro perteneciente al patrimonio cultural de la Nación.

> 4. El máximo de la pena de prisión será de CINCO (5) años cuando el daño:
>
> a. Pusiere en peligro la vida, la integridad física o la salud de una o más personas.
> b. Consistiere en la violación o destrucción de tumbas, con o sin esparcimiento de cadáveres, motivada en razones discriminatorias.
>
> 5. Se impondrá la pena de prisión de SEIS (6) meses a UN (1) año o multa de DIEZ (10) a CIEN (100) días, al que indebidamente realizare u ordenare realizar tareas de prospección, remoción o excavación en yacimientos arqueológicos y paleontológicos, cuando no resultare daño."

Esta versión final suprime el párrafo segundo del actual art. 183, en cuanto refiere a que se considera daño a bienes intangibles descripto a través de datos, documentos, programas y sistemas, como refería en su redacción "En la misma pena incurrirá el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos".

No obstante si mantiene como figura típica de venta distribución, puesta en circulación o introducción en un sistema informático, cualquier programa destinado a causar daños.

4.6 | El tipo penal de interrupción o entorpecimiento de las comunicaciones

La reforma de la ley 26.388 previó la interrupción o entorpecimiento de las comunicaciones como una de las conductas que podían realizarse a través de medios informáticos o dispositivos digitales. Así fue como la reforma introdujo al texto original de este tipo penal la expresión "comunicación (…) de otra naturaleza", a fin de abarcar las comunicaciones electrónicas en general.

De esta manera, el art. 197 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".

La Comisión de Reforma, Actualización e Integración del Código Penal de la Nación había efectuado una pequeña modificación terminológica a la conducta típica descripta, sustituyendo la expresión "comunicación (…) de otra naturaleza", por "toda comunicación transmitida por cualquier medio alámbrico o inalámbrico", lo cual resultaba más extensivo y preciso.

Sin embargo, la versión final y definitiva del Anteproyecto de Ley de Reforma, Actualización e Integración del Código Penal de la Nación deja redactado, en el art. 190, el tipo penal de interrupción de comunicaciones de la siguiente manera:

> "1. El que, sin crear una situación de peligro común, impidiere o interrumpiere el normal funcionamiento de los transportes por tierra, agua o aire, 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, será reprimido con prisión de SEIS (6) meses a DOS (2) años.
>
> 2. En caso de impedimento o interrupción de servicios de transporte por tierra, agua o aire, el delito solo se configurará mediante desobediencia a la pertinente intimación judicial."

La redacción definitiva del tipo abandona la descripción original de la conducta típica pero contempla la interrupción "telefónica, radiofónica, satelital o electrónica", sustituyendo así la expresión comunicación (...) de otra naturaleza".

La escala pena no es alterada, manteniéndose la pena de seis (6) meses a dos (2) años de prisión.

4.7 | El tipo penal de alteración, sustracción, ocultación, destrucción e inutilización de medios de prueba

La ley 26.388 previó también como tipo penal que pudiera ser realizado por medios informáticos la alteración, sustracción, ocultamiento, destrucción e inutilización de los medios de prueba, en el art. 255 CP:

> "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, este será reprimido con multa de pesos setecientos cincuenta ($ 750) a pesos doce mil quinientos ($ 12.500)".

En el primer borrador de trabajo se había mantenido la redacción original de la ley 26.388 alterando únicamente, para el caso de la conducta negligente o culposa, la pena por días multa en el caso de tope máximo de la escala prevista para el delito imprudente, lo que puede verificarse en el texto transcripto a continuación.

> "Será reprimido con prisión de un (1) mes a cuatro (4) años, el que sustrajere, ocultare, destruyere o inutilizare objetos destinados a servir de prueba ante la autoridad competente, registros o documentos confiados a la custodia de un funcionario o de otra persona en el interés del servicio público.
>
> Si el culpable fuere el mismo depositario, sufrirá además inhabilitación especial por el doble del tiempo de la condena.
>
> Si el hecho se cometiere por imprudencia o negligencia del depositario, este será reprimido con multa de sesenta (60) a trescientos sesenta (360) días-multa".

Sin embargo en su versión final y definitiva, la figura ha quedado contemplada en el art. 260, con la siguiente redacción:

> "1. Será reprimido con prisión de SEIS (6) meses a CUATRO (4) años, el que sustrajere, ocultare, alterare, destruyere o inutilizare objetos destinados a servir de prueba ante la autoridad competente, registros o documentos confiados a la custodia de un funcionario o de otra persona en el interés del servicio público.

> 2. Si el culpable fuere el mismo depositario, sufrirá además inhabilitación por el doble de tiempo de la condena.
>
> 3. Si el hecho se cometiere por imprudencia o negligencia del depositario, éste será reprimido con multa de TREINTA (30) a CIENTO OCHENTA (180) días."

En la versión final y definitiva del Anteproyecto se mantiene la redacción original del tipo penal de alteración, sustracción, ocultamiento, destrucción e inutilización de medios de prueba.

Solo se incrementa el mínimo de la pena de un mes a seis (6) meses para el tipo penal doloso. En cuanto al tipo culposo, se estable días multas en lugar una suma pecuniaria.

5 | Recomendaciones y sugerencias

Hace tan solo dos años atrás, en junio del año 2011 más precisamente, nos referimos puntualmente a las ventajas y limitaciones político-criminales de la Reforma al Código Penal de la Nación en materia de criminalidad informática establecida por la ley 26.388.[32] En esta oportunidad es menester profundizar este análisis debido a la incorporación de las recientes leyes 26.685, 26.904 y al actual Anteproyecto de Ley de Reforma, Actualización e Integración del Código Penal de la Nación (decreto 678/2012).

Como expresáramos oportunamente, "la ley 26.388 de ciberdelitos constituye un gran avance legislativo, sobre todo por su ambición de reformar integralmente y actualizar el Código Penal...".[33] y desde una perspectiva de la técnica legislativa empleada, el legislador ha acudido a la instrumentación de una ley de reforma integral, armónica y concordada al Código Penal de la Nación.

(32) Sueiro, Carlos C., "La eficiencia de la reforma en materia de criminalidad informática", ponencia presentada y galardonada con el Segundo lugar en el XI Encuentro de la Asociación Argentina de Profesores de Derecho Penal, Facultad de Derecho de la Universidad Nacional de Rosario, Provincia de Santa Fe, 1°, 2° y 3° de junio de 2011, en *La Ley*, Suplemento de Penal y Procesal Penal, 2011, pp. 11/22.

(33) Reggiani, Carlos, *Delitos Informáticos*, Bs. As., *La Ley*, 2008-D, p. 1090.

Ella no implicó la creación nuevas figuras delictivas o tipos penales, sino que se modificaron ciertos aspectos de los tipos penales ya contemplados por nuestro ordenamiento jurídico con el objeto de receptar y captar las nuevas tecnologías como medios comisivos para su ejecución, afirmando así que las TIC solo constituyen nuevos medios comisivos para realizar las acciones ya descriptas por los tipos penales previstos por nuestro Código Penal.

Así, con esta reforma se incorporaron los tipos penales de:

1. Ofrecimiento y distribución de imágenes relacionadas con pornografía infantil (art. 128 CP),
2. Violación de correspondencia electrónica (art. 153 CP),
3. Acceso ilegítimo a un sistema informático (art. 153 *bis* CP),
4. Publicación abusiva de correspondencia (art. 155 CP),
5. Revelación de secretos (art. 157 CP),
6. Delitos relacionados con la protección de datos personales (art. 157 *bis* CP),
7. Defraudación informática (art. 173, inc. 16 CP),
8. Daño (arts. 183 y 184 CP),
9. Interrupción o entorpecimiento de las comunicaciones (art. 197 CP),
10. El tipo penal de alteración, sustracción, ocultación, destrucción e inutilización de medios de prueba (art. 255 CP).

Debe destacarse, como menciona Riquert, que "la ley 26.388 ha significado un sustancial avance sobre temas cuya consideración venía siendo reclamada desde mucho tiempo atrás, poniendo fin a antiguas discusiones jurisprudenciales y doctrinarias".[34]

Asimismo, la ley 26.388 también ha seguido los lineamientos establecidos por el "Convenio sobre la Ciberdelincuencia de Budapest",[35] incorporando las definiciones terminológicas en el art. 77 CP, teniendo en consideración las definiciones suministradas por el Convenio arriba citado en su art. 1° destinado a "Definiciones", perteneciente al Capítulo I, dedicado a la "Terminología".

(34) Riquert, Marcelo A., *Delincuencia Informática en Argentina y el Mercosur*, Bs. As., Ediar, 2009, p. 217.

(35) Ver "Convenio sobre la ciberdelincuencia", Budapest, 23/11/2001, [en línea] http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Convention%20and%20protocol/ETS_185_spanish.PDF.

Otra ventaja desde una perspectiva criminológica de la ley 26.388 es que no ha recurrido en tal sentido a una clasificación biotipológica o en este caso puntual, cibertipológica de autores. En este sentido, la presente ley 26.388 en ninguno de los tipos penales contemplados ha recurrido al empleo de una biotipología de autores de la criminalidad informática o cibertipología como puede ser las designaciones de: 1) *hacker*; 2) *cracker*; 3) *preaker* o *phreaker*; 4) *phisher*; 5) *sniffer*; 6) *virucker*; 7) propagandista informático, 8) pirata informático, o 9) *cyberbullying* o ciber-acosador.

Asimismo, a nivel dogmático, también debe elogiarse que la mayoría de los tipos penales que han sido modificados son tipos penales dolosos, no presentando el empleo de tipos penales culposos a excepción del tipo penal de alteración, sustracción, ocultación, destrucción e inutilización de medios de prueba (art. 255 CP), y no habiéndose incorporado ningún tipo omisivo, ni doloso, ni culposo, lo cual debe destacarse en un Estado de Derecho, y respetuoso del principio de reserva de los ciudadanos.

No obstante, nuestro actual sistema normativo en materia de criminalidad informática presenta múltiples limitaciones en materia penal, procesal penal, infraestructura y capacitación de la administración de justicia, y cooperación internacional.

5.1 | La actualización normativa en materia de criminalidad informática

Nuestro actual sistema normativo en materia de criminalidad informática, si bien presenta todas las ventajas que hemos referido previamente, también exhibe limitaciones y deficiencias en diversas materias.

5.5.1. Recomendaciones y sugerencias de actualización en materia de Derecho Penal

En primer lugar, debemos referir que pese a que ley 26.388 constituyó una ley de reforma integral y concordada al Código Penal de la Nación y que implicó la modificación de varios de los tipos penales tradicionales, desgraciadamente esta reforma no abarcó o comprendió todas las figuras delictivas que pueden perpetrarse a través de medios informáticos o dispositivos electrónicos. Se sugiere, sin renunciar a una política criminal reductora del poder punitivo, la incorporación de los siguientes tipos penales.

5.5.1.1. Tipos penales propuestos por otros proyectos de ley previos, no incorporados por las leyes 26.388, 26.904, ni por el Anteproyecto (decreto 678/2012)

a. El tipo penal de hurto (art. 162 CP);[36]

b. El tipo penal de revelación de secretos de Estado y ultraje a los símbolos patrios (art. 222 CP);[37]

c. El tipo de penal de incendios y otros estragos (art. 186 CP);[38]

d. Los tipos penales de falsificación de documento público y privado (art. 292 CP) y uso de documento falso o adulterado (art. 296 CP).[39]

5.5.1.2. Tipos penales previstos en leyes complementarias y no incorporados por las leyes 26.388, 26.904, ni por el Anteproyecto (PEN, decreto 678)

a. El Régimen Penal Tributario (leyes 24.769 y 26.735),

b. El Régimen Penal Cambiario (leyes 19.359, 22.338, 23.928, 24.144 y decreto 480/1995),

c. El Derecho Penal Aduanero (ley 22.415)[40]

(36) Figura esta que había sido propuesta para permitir su perpetración o realización a través de medios informáticos o tecnologías digitales en tres proyectos de ley. En el año 1996 fue objeto de tratamiento de los Proyectos de ley del Diputado Carlos R. Álvarez y del Proyecto del Diputado José A. Romero Feris, este último a su vez presentado también en el año 2000 cuando Romero Feris se desempeñaba como senador bajo el número de expediente 0168-S-2000 ante la Honorable Cámara de Senadores del Congreso de la Nación, sin que el mismo lograra ser aprobado por ambas cámaras del Congreso de la Nación.

(37) El tipo penal que cobra significativa importancia luego del "caso Wikileaks". Véase Iellimo, Marcela, "El caso Wikileaks ¿un planteo de cambio para el orden jurídico internacional?", [en línea] *elDial.com*, DC1522; Domscheit-Berg, Daniel, *Dentro de WikiLeaks. Mi etapa en la web más peligrosa del mundo*, (trads. Ana Duque de Vega y Carles Andreu Saburit), Bs. As., Rocaeditorial, 2011; y O´Donnell, Santiago, *ArgenLeaks*, Bs. As., Sudamericana, 2011.

(38) Tipo penal propuesto por el Proyecto de Ley de la Diputada Leonor E. Tolomeo en 1996.

(39) En lugar de dejarlo supeditado a la interpretación extensiva, ambas figuras se encuentran alcanzadas por las modificaciones de terminología previstas en el art. 77 CP. Palazzi, Pablo A., *Los Delitos Informáticos en el Código Penal. Análisis de la ley 26.388*, Bs. As., Abeledo-Perrot, 2009, pp. 35/36.

(40) "Sería importante que para evitar los perniciosos efectos de la descodificación, como la falta de coherencia, de armonía y pérdida de proporcionalidad (...) se asumiera la profundiza-

5.5.1.3. La incorporación de nuevos tipos penales

A criterio de autores como Riquert y Palazzi, debieron ser tratadas en forma más exhaustiva por la reforma para decidir su incorporación o exclusión los siguientes tipos penales:

a. La ciberocupación o registro impropio de nombres de dominio,(41)

b. El *spamming* o correo basura o publicidad no solicitada,(42)

c. La captación ilegal y difusión de datos, imágenes y sonidos,(43)

d. La posesión simple de material pornográfico infantil,

e. La responsabilidad de los proveedores.(44)

5.5.2. Recomendaciones y sugerencias de actualización en materia de Derecho Procesal Penal

Otra limitación es que, a la fecha, pese la sanción de las leyes 26.388, 26.685, 26.904 y la presentación del Anteproyecto de Ley de Reforma, Actualización e Integración del Código Penal de la Nación, no se cuenta con una reforma a nivel procesal penal en materia de criminalidad informática.

ción de la técnica de la última reforma (...) al que faltaría incorporar los tipos penales que en leyes especiales han quedado aislados, mejorando así su sistematicidad y orden", en Riquert, Marcelo A., *Delincuencia Informática..., op. cit.*, p. 218.

(41) Riquert, *ibid.*, pp. 202/204.

(42) *Ibid.*, pp. 204/206.

(43) Palazzi, Pablo A., *Los Delitos Informáticos..., op cit.*, pp. 159/166, quien se inclina por su no punición y su amparo a través del Derecho Civil. También Riquert, Marcelo A., *Delincuencia Informática..., op. cit.*, pp. 206/207, quien considera prudente y acertado postergar su punición hasta que exista un serio debate en torno a esta figura penal.

(44) Tomeo, Fernando, *Responsabilidad penal de los administradores de sitios web. El "caso Taringa!"*, Bs. As., La Ley, 01/06/2011; Granero, Horacio R., "La naturaleza jurídica de la nube *('cloud computing')*", [en línea] *elDial.com*, DC11A9; Velazco San Martín, Cristo, "Aspectos jurisdiccionales de la computación de la nube", [en línea] *elDial.com*, DC1304; Elizalde Marín, Francisco, "La prueba en la *Cloud Computing: Cloud Computing & Service Level Agreements*. El modelo en los Estados Unidos de América y su proyección al ámbito local argentino", [en línea] *elDial.com*, DC15EE; Teijeiro, Nicolás, "La protección constitucional de la intimidad en internet con especial referencia a redes sociales", [en línea] *elDial.com*, DC15EF.

Se sugiere o recomienda la adaptación de nuestra legislación procesal penal a la Sección 2 del "Convenio sobre la Ciberdelincuencia de Budapest" destinada al derecho procesal.[45]

Así, resultaría indispensable que una legislación procesal penal en materia de criminalidad informática prevea:

1. La conservación rápida de datos informáticos almacenados (art. 16 del Convenio);
2. Conservación y revelación parcial rápidas de los datos relativos al tráfico (art. 17 del Convenio);
3. Orden de presentación (art. 18 del Convenio);
4. Registro y confiscación de datos informáticos almacenados (art. 19 del Convenio);
5. Obtención en tiempo real de datos relativos al tráfico (art. 20 del Convenio); y
6. Interceptación de datos relativos al contenido (art. 21 del Convenio).

5.5.3. Recomendaciones y sugerencias para la actualización de la infraestructura tecnológica y capacitación del personal de la administración de justicia

En directa relación con la ausencia de la sanción de una ley procesal penal en materia de criminalidad informática, debemos referir la carencia de órganos especializados dentro del sistema de administración de justicia (Poder Judicial de la Nación,[46] Ministerio Público Fiscal[47] y Ministerio Pú-

(45) "La reforma legislativa reviste una importancia central frente a la necesidad de readecuar las normas procesales, (...) ante el avance del ciberdelito y la falta de previsión legislativa ante las extendidas formas delictivas. (...) La necesidad de reformular las reglas procesales sobre prueba digital se torna imperiosa, ya que si bien el uso de la analogía probatoria está permitida en materia procesal, resulta evidente la inconveniencia de seguir utilizando normas destinadas a otras situaciones (por ejemplo, intervenciones telefónicas) a realidades nuevas y con distintas connotaciones (por ejemplo, intervenciones de cuentas de correo electrónico)". Sáenz, Ricardo y Ruiz, Maximiliano, "Hacia un nuevo modelo de investigación en materia de ciberdelincuencia", [en línea] *elDial.com*.

(46) El Poder Judicial de la Nación, por medio de la CSJN ha realizado profundas actualizaciones en materia de infraestructura tecnológica y capacitación del personal. Lo cierto es que en la actualidad no se cuenta con ningún Juzgado Nacional especializado en materia de criminalidad informática o área destinada específicamente a esta materia. Ver CSJN, *Justicia argentina* online, [en línea] http://www.fam.org.ar/media/img/paginas/Justicia%20Argentina%20On%20Line.pdf.

(47) Desgraciadamente, el Ministerio Público Fiscal se encuentra en una situación análoga a la del Poder Judicial de la Nación, ya que si bien cuenta con un importante número de

blico de la Defensa)[48] y sus auxiliares (Policía Federal Argentina —PFA—, Gendarmería Nacional Argentina —GNA—, Prefectura Naval Argentina —PNA—, y la Policía de Seguridad Aeroportuaria —PSA—).

Se recomienda y sugiere:

a. La creación de juzgados, fiscalías y defensorías especializadas en materia de criminalidad informática o delitos de alta tecnología.[49]

b. La capacitación del personal para afrontar el gran desafío que implica la digitalización e informatización de la administración de justicia a partir de la sanción de la ley 26.685.

c. Capacitar y concientizar sobre otro nuevo fenómeno no contemplado o previsto por las leyes 26.388, 26.685, 26.904 y por el Anteproyecto de Ley de Reforma, Actualización e Integración del Código Penal de la Nación, que ha surgido de la revolución digital y de la computación de la nube o *cloud computing*.[50]

Unidades Fiscales Temáticas o Unidades Especiales, hasta la fecha no ha creado o destinado recursos a instaurar una Unidad Fiscal especializada en criminalidad informática. Véase www.mpf.gov.ar.

(48) Idéntica realidad exhibe el Ministerio Público de la Defensa (MPD), quien también posee una gran cantidad de Comisiones y Programas, como así también un importante Departamento de Informática dentro del área de la Dirección General de Administración de la Defensoría General de la Nación, pero hasta el presente no dispone de ninguna comisión o programa especializado en criminalidad informática. Fuente [en línea] www.mpd.gov.ar.

(49) Como bien refieren el Fiscal General Dr. Ricardo Sáenz y el funcionario Dr. Maximiliano Ruiz al manifestar que "el Ministerio Público Fiscal, como actor y motor principal de las investigaciones [debe] enfrentar esta problemática mediante un lineamiento estratégico político criminal". Es así como proponen trazar "dos puntos de aproximación en materia de investigaciones sobre ciberdelicuencia, a saber: 1) una amplia reforma legislativa a nivel procesal actualizadora de las normas sobre investigación en esta materia, y 2) la creación de una Fiscalía especial integral e interdisciplinaria dedicada a la investigación de los delitos informáticos", ver Sáenz, Ricardo y Ruiz, Maximiliano, "Hacia un nuevo modelo de investigación en materia de ciberdelincuencia", [en línea] *elDial.com.*, DC19CB.

(50) Esta tecnología de la "computación de la nube" (*cloud computing)* presenta serios problemas de compatibilidad con la implementación del expediente digital. En primer lugar, porque la computación de la nube o *cloud computing*, "por su naturaleza distribuida [en forma de] nube informática a menudo empaña su ubicación y las medidas de seguridad asociada a los datos (...) Esta situación en particular, choca con los requisitos legales de protección de datos". En el caso puntual de la implementación del expediente digital por parte de la administración de justicia, deberá tenerse en consideración que si se desea hacer uso de la tecnología de la computación de la nube o *cloud computing*, la CSJN deberá pensar en el empleo de una "nube privada" (*private cloud*), ya que el uso de una "nube pública" (*public cloud*) o "nube híbrida" o "multi nube" (*hybrid cloud* o *multi cloud*), traerá aparejado un sin número de riesgos, tales como la pérdida de la privacidad y protección de datos personales, la pérdida del control de la información personal, el desconocimiento de la localización y ubicación de la in-

5.5.4. Recomendaciones y sugerencias para la actualización en materia de cooperación internacional

a. Profundizar el estudio de los problemas en materia de criminalidad informática que trae aparejada para la aplicación espacial de la ley penal, sin adaptar nuestra legislación nacional a la Sección 3 del "Convenio sobre la Ciberdelincuencia de Budapest" destinada a la "Jurisdicción".

b. Contemplar la protección de un bien jurídico colectivo, macrosocial o supraindividual, como por ejemplo la hipotética protección del "ciberespacio público", "medio ambiente digital" o "espacio virtual público".[51]

6 | Conclusión

El presente trabajo ha buscado exponer las disposiciones legales vigentes a nivel nacional en materia de criminalidad informática y las actualizaciones y reformas que se han propuesto a través de la presentación el Anteproyecto de Ley de Reforma, Actualización e Integración del Código Penal de la Nación.

Asimismo, hemos apreciado las exigencias y cambios significativos que se han producido en todas nuestras expresiones culturales desde los inicios de la sociedad de la información del siglo XXI y cómo ella plantea nuevos retos al momento de concebir e instrumentar normales legales, infraestructura tecnológica y capacitación eficiente para adecuar nuestra

formación, problemas con la transmisión o flujo transfronterizo de datos, destrucción o alteración de datos, divulgación de datos, acceso no autorizado a datos, alto nivel de vulnerabilidad, o posible indisponibilidad de la información por falta de conectividad.

(51) Muy probablemente por el hecho de desconocer que el acceso a las nuevas tecnologías de la información y comunicación (TIC) así como a Internet hoy han adquirido el estatus o nivel de derechos humanos gracias a la "Declaración Universal de los Derechos Humanos Emergentes" (DUDHE) elaborada en el "Fórum Universal de las Culturas Barcelona 2004" y aprobada en el "Fórum de las Culturas de Monterrey 2007", como así también por el informe de Naciones Unidas que pone en cabeza de todos los estados el garantizar el acceso a Internet toda vez que constituye un nuevo derecho humano indispensable para la concreción de otros derechos humanos, como la libertad de expresión. Considerar el acceso a *web* y a las nuevas tecnologías digitales como un derecho humano emergente constituye el marco jurídico sobre el cual en unos pocos años podrá sustentarse la construcción de un bien jurídico colectivo, supraindividual y macrosocial como lo puede ser el "ciberespacio público", "medio ambiente digital" o "espacio virtual público", en pos de resguardar todas las actividades sociales que dependen directa o indirectamente del correcto funcionamiento de sus sistemas informáticos públicos interconectados vía Internet y también a través de intranet. Véase Carnevale, Carlos A., "¿El acceso a internet es un Derecho Humano?", [en línea] *elDial.com.*, DC1746.

administración de justicia actual a los requerimientos de una sociedad altamente informatizada.

A lo largo del estudio y tras analizar las propuestas de actualización y reforma en materia de criminalidad informática propuestas por el Anteproyecto de Ley de Reforma, Actualización e Integración del Código Penal de la Nación, hemos realizados recomendaciones y sugerencias en torno a la actualización de la ley penal, procesal penal, cooperación internacional e infraestructura tecnológica y capacitación del personal de la administración de justicia en materia de criminalidad informática.

Es así como sugerimos entre las reformas a instrumentarse en el área del derecho penal la incorporación de tipos penales tales como:

1. El hurto (art. 162 CP),
2. El tipo pena de revelación de secretos de Estado y ultraje a los símbolos patrios (art. 222 CP),
3. Incendios y otros estragos (art. 186 CP),
4. Los tipos penales de falsificación de documento público y privado (art. 292 CP) y uso de documento falso o adulterado (art. 296 CP);
5. El Régimen Penal Tributario (leyes 24.769 y 26.735),
6. El Régimen Penal Cambiario (leyes 19.359, 22.338, 23.928 y 24.144 y decreto 480/1995);
7. El Derecho Penal Aduanero (ley 22.415),
8. La ciberocupación o registro impropio de nombres de dominio,
9. El *spamming* o correo basura o publicidad no solicitada,
10. La captación ilegal y difusión de datos, imágenes y sonidos,
11. La responsabilidad de los proveedores.

En lo que respecta a las reformas a instrumentarse a nivel de derecho procesal penal, se sugirió la indispensable adaptación de nuestra legislación procesal penal a la Sección 2 del "Convenio sobre la Ciberdelincuencia de Budapest" destinada al "Derecho Procesal".

Acompañándose esta reforma procesal penal con actualización de la infraestructura tecnológica y capacitación del personal de la administración de justicia que impliquen la creación de juzgados, fiscalías y defensorías especializadas en materia de criminalidad informática o delitos de alta

tecnología, la capacitación del personal para afrontar el gran desafío que implica la digitalización e informatización de la administración de justicia a partir de la sanción de la ley 26.685, y concientización sobre el nuevo fenómeno la computación de la nube o *cloud computing*.

Finalmente, también se sugirió, en materia de cooperación internacional, profundizar seriamente en el estudio de los problemas en materia de criminalidad informática que trae aparejado para la aplicación espacial de la ley penal, adaptando nuestra legislación nacional a la Sección 3 del "Convenio sobre la Ciberdelincuencia de Budapest" destinada a la jurisdicción; y la contemplación de una posible futura protección de un bien jurídico colectivo, macrosocial o supraindividual, como por ejemplo la hipotética protección del "ciberespacio público", "medio ambiente digital" o "espacio virtual público".

Todo ello en aras de contar con una normativa legal en materia penal, procesal penal y en el área de cooperación internacional acordes a los desafíos que plantea el traspaso a una sociedad altamente tecnificada.

Congresos y Seminarios

Coloquios preparatorios para el XIX Congreso Internacional de Derecho Penal:

"Sociedad de la Información y Derecho Penal"

(AIDP, Río de Janeiro, Brasil, 31 de agosto al 6 de septiembre 2014)

Las preguntas de estas secciones tratan generalmente del ciberdelito.

Se trata de un cuestionario formulado a abogados penalistas de todos los países, sobre el tema de los delitos informáticos.

Por Argentina respondieron los Dres. Javier Augusto De Luca, Marcelo Riquert, Christián C. Sueiro, María Ángeles Ramos y Francisco Figueroa.

Se trata de dar cobertura a las conductas criminales que afectan a intereses asociados con el uso de la tecnología de la información y comunicación (TIC), como el funcionamiento adecuado de los sistemas informáticos y de Internet, la intimidad y la integridad de los datos almacenados o transferidos a, o a través de, las TIC o la identidad virtual de los usuarios de Internet.

El denominador común y rasgo característico de todas las figuras de ciberdelitos y de la investigación sobre éstos puede hallarse en su relación con sistemas, redes y datos de ordenadores, de un lado, y con los sistemas, redes y datos cibernéticos, del otro.

El ciberdelito cubre delitos que tienen que ver con los ordenadores en sentido tradicional y también con la nube del ciberespacio y las bases de datos cibernéticas.

Sección I

Relator General: **THOMAS WEIGEND**[1]

Grupo Nacional Argentino: **JAVIER AUGUSTO DE LUCA, MARCELO RIQUERT, CHRISTIÁN C. SUEIRO, MARÍA ÁNGELES RAMOS** y **FRANCISCO FIGUEROA**

Nótese que en este cuestionario solo son de interés las cuestiones relativas a las características generales de las tipificaciones de las figuras delictivas del ciberdelito. Las cuestiones específicas concernientes a las definiciones de figuras individuales serán objeto de debate en la Sección II del Congreso.

I | Criminalización

1.1. ¿Qué bienes jurídicos específicos se considera que deben ser protegidos por el derecho penal (p. ej., integridad de los sistemas procesadores de datos, privacidad de los datos almacenados)?

La legislación de la República Argentina en materia de criminalidad informática, en particular la ley 26.388, no creó bienes jurídicos autónomos o específicos de delitos informáticos.

Los bienes jurídicos que han sido alcanzados por la reforma son:

1. Delitos contra la integridad sexual;
2. Delitos contra la libertad, específicamente la violación de secretos y de la privacidad;
3. Los delitos contra la propiedad (antes, también por ley 25.930/04);
4. Los delitos contra la Seguridad Pública;
5. Delitos contra la Administración Pública.

(1) Por dudas y consultas dirigirse al Relator General Profesor Dr. Thomas Weigend: thomas.weigend@uni-koeln.de

Así, a partir de su reforma, la ley 26.388 alcanzó un número muy limitado y específico de tipos penales, como son:

1. El ofrecimiento y distribución de imágenes relacionadas con pornografía infantil (art. 128 del Código Penal, en adelante CP);
2. Violación de la correspondencia electrónica (art. 153 CP);
3. Acceso ilegítimo a un sistema informático (art. 153 *bis* CP);
4. Publicación abusiva de correspondencia (art. 155 CP);
5. Revelación de secretos (art. 157 CP);
6. Delitos relacionados con la protección de datos personales (art. 157 *bis* CP);
7. Defraudación informática (art. 173, inc. 16, CP);
8. Daño (art. 183 y 184, CP);
9. Interrupción o entorpecimiento de las comunicaciones (art. 197 CP);
10. El tipo penal de alteración, sustracción, ocultación, destrucción e inutilización de medios de prueba (art. 255 CP), a lo cual deben agregarse las modificaciones terminológicas realizadas en el art. 77 CP.

Además, a través de modificaciones e inserciones en leyes especiales, se han considerado otros bienes jurídicos, a saber:

1. Secreto empresarial (por ley 24.766/97);
2. Hacienda pública (por leyes 24.769/97 y 26.735/11);
3. Propiedad intelectual (por ley 25036/98);
4. Servicios de comunicaciones móviles (por ley 25.891/04).

1.2. Por favor, dar ejemplos típicos de leyes penales relativas a los siguientes delitos

1.2.1. Ataques contra sistemas TIC

Puntualmente se contempla el ataque a los sistemas informáticos tanto tangibles (hardware) e intangibles (software) en el tipo penal de daño simple y agravado (arts. 183 y 184 CP).

En similar dirección, se contempla la alteración dolosa de registros fiscales y la adulteración de controladores fiscales (arts. 12 y 12 *bis* de la ley 24.769); la alteración de número de línea, de número de serie electrónico o mecánico del equipo terminal o módulo de identificación removible de usuario de SCM; la alteración de componente de una tarjeta de telefonía, el

acceso a los códigos informáticos de habilitación de créditos de servicio SCM o el aprovechamiento ilegítimo de estos últimos (arts. 10 y 11, ley 25.891).

1.2.2. Violación de la privacidad TIC

Específicamente, el Código Penal de la Nación Argentina previó en su título "Violación de Secreto y de la Privacidad" los siguientes tipos penales:

1. Violación de correspondencia electrónica (art. 153 CP);
2. Acceso ilegítimo a un sistema informático (art. 153 *bis* CP);
3. Publicación abusiva de correspondencia (art. 155 CP);
4. Revelación de secretos (art. 157 CP).
5. Delitos relacionados con la protección de datos personales (art. 157 *bis* CP)

Los arts. 2 y 12 de la ley 24.766/97 protegen la violación de la confidencialidad sobre información y productos que estén legítimamente bajo control de una persona y se divulgue indebidamente, de manera contraria a los usos comerciales honestos.

1.2.3. Falsedad *forgery* y manipulación de los datos almacenados digitalmente

Puntualmente se prevé la figura "defraudación informática" (art. 173, inc. 16, CP), que es más específica que la de "defraudación a sistemas automatizados o con tarjetas de crédito y débito" (art. 173, inc. 15 CP).

1.2.4. Distribución de virus de ordenadores

El tipo penal de daño previsto en el art. 183, 2° párr. CP, prevé como conducta típica "la venta, distribución, puesta en circulación o introducción en un sistema informático, de cualquier programa destinado a causar daños".

1.2.5. Delitos relativos a las identidades virtuales de los usuarios, p. ej., *forging,* sustracción o daño de personalidades virtuales

No existe una figura específica, pero cualquier adulteración de datos personales puede quedar subsumida en los delitos relacionados con la protección de datos personales (art. 157 *bis* CP).

El 13/05/2010, por disposición 7/2010, la Dirección Nacional de Protección de Datos Personales creó el "Centro de Asistencia a las Víctimas de Robo de Identidad".

1.2.6. Otras prohibiciones penales innovadoras en el área de las TIC y de Internet, p. ej., incriminación de la creación y posesión de ciertas imágenes virtuales, violación de derechos de autor en la esfera virtual

La producción, financiación, ofrecimiento, comercialización, publicación, facilitación, divulgación y distribución de imágenes de toda representación de actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales en el que participaren menores (art. 128 CP).

La defraudación de derechos de propiedad intelectual está prevista en el art. 71 y ss. de la ley 11.723 (ver modificaciones introdicudas por ley 25.036/98).

1.3. ¿Cómo se define típicamente la conducta criminal (*actus reus*) en estos delitos (describiendo el acto, el resultado, otros)? ¿Cómo se define el objeto ("dato", "escritos", contenidos)?

El legislador ha sido muy respetuoso del principio de legalidad y, en la mayoría de los tipos penales, ha descripto la conducta o acción típica.

Desde una perspectiva criminológica, la ley 26.388, de reforma en materia de criminalidad informática al Código Penal de la Nación, no exhibe una remisión terminológica y conceptual a la Escuela Positivista de la Criminología; no ha recurrido, en tal sentido, a una clasificación "biotipológica" o, en este caso puntual, "cibertipológica" de autores.

Es decir, la presente ley 26.388, en ninguno de los tipos penales contemplados, ha recurrido al empleo de una biotipología de autores de la criminalidad informática o cibertipología, como pueden ser las designaciones de: 1) *Hacker*;[2] 2) *Cracker*;[3] 3) *Preaker* o *Phreaker*;[4] 4) *Phisher*;[5]

(2) Ver Chiaravalloti Alicia y Ricardo Levene (h.), "Delitos informáticos. Segunda Parte", en *La Ley* 1998-F, 976; Fillia, Leonardo C.; Monteleone, Romina; Nager, Horacio S.; Sueiro, Carlos C., *Análisis integrado de la Criminalidad Informática*, prólogo de Carlos Alberto Elbert, Bs. As., Editorial Fabián J. Di Plácido, 2007, p. 117; Tobares Catalá, Gabriel H. ; Castro, Argüello Maximiliano J., *Delitos Informáticos*, prólogo de Marcelo J. Sayago, Córdoba, Advocatus, 2010, p. 97.

(3) Ver Chiaravalloti Alicia y Ricardo Levene (h.), *ibid.*; Fillia, Leonardo C.; Monteleone, Romina; Nager, Horacio S.; Sueiro, Carlos C., *ibid.*, p. 118; Tobares Catalá, Gabriel H. ; Castro, Argüello Maximiliano J., *ibid.*, p. 99.

(4) Ver Chiaravalloti Alicia y Ricardo Levene (h.), *ibid.*; Fillia, Leonardo C.; Monteleone, Romina; Nager, Horacio S.; Sueiro, Carlos C., *ibid.*, p. 118.

(5) Ver Fillia, Leonardo C.; Monteleone, Romina; Nager, Horacio S.; Sueiro, Carlos C., *ibid.*, p. 119.

5) *Sniffer*;[6] 6) *Virucker*;[7] 7) Propagandista informático;[8] 8) Pirata Informático;[9] o 9) *Cyberbullyng* o Ciber-Acosador.

La mayoría de los tipos penales son tipos penales de resultado; por ejemplo, daño, defraudación, interrupción de comunicaciones, etc.

Sin perjuicio de la utilización de referencias al objeto como "datos", "documentos", "información registrada", en la parte general del Código se incorporaron, por la ley 26.388, estos tres últimos párrafos al art. 77 CP:

> "El término documento comprende toda representación de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión.
>
> Los términos firma y suscripción comprenden la firma digital, la creación de una firma digital o firmar digitalmente.
>
> Los términos instrumento privado y certificado comprenden el documento digital firmado digitalmente".

1.4. La responsabilidad penal por ciertos ciberdelitos, ¿se limita a determinados grupos de autores y/o víctimas?

Nuestra legislación penal no posee tipos penales con sujetos activos calificados o grupos de autores.

No obstante, la calidad personal del agente puede operar como calificante. Así, en el art. 157 *bis* CP, cuando el autor del delito sea funcionario público sufrirá, además, pena de inhabilitación especial. La ley 25.891 establece un agravante genérico que incrementa las penas mínimas y máximas en un tercio: la autoría por dependientes de empresas licenciatarias de SCM o por quienes, atento al desempeño de sus funciones, posean acceso a las facilidades técnicas de aquéllas.

(6) Rosende Eduardo E., "El intrusismo informático. Reflexiones sobre su inclusión en el Código Penal", en *Suplemento La Ley Penal y Procesal Penal*, Bs. As., La Ley, 27/05/2008, p. 21.

(7) Ver Riquert Marcelo Alfredo, *Informática y Derecho Penal Argentino*, Bs. As., Ad-Hoc, 1999, p. 57; Fillia, Leonardo C.; Monteleone, Romina; Nager, Horacio S.; Sueiro, Carlos C., *op. cit.*, p. 120; Tobares Catalá, Gabriel H. ; Castro, Argüello Maximiliano J., *op. cit.*, p. 101.

(8) Riquert Marcelo A., *ibid.*, p. 57; Fillia, Leonardo C.; Monteleone, Romina; Nager, Horacio S.; Sueiro, Carlos C., *op. cit.*, p. 120.

(9) Ver Riquert Marcelo A., *ibid.*, p. 57.

Respecto de las víctimas, solo se destaca la protección de los menores en lo concerniente a la venta, producción, difusión, facilitación y publicidad de material pornográfico.

En el art. 153 *bis* CP se califica (agrava) la conducta de intrusismo 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.

A su vez, el art. 184 CP considera agravado el daño cuando recae sobre datos, documentos, programas o sistemas informáticos públicos (inc. 5) o 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 (inc. 6).

1.5. ¿Se extiende la responsabilidad penal en el área de las TIC a las conductas meramente imprudentes o negligentes?

La legislación penal argentina posee un tipo penal imprudente en materia de criminalidad informática.

Este tipo penal doloso abarca la alteración, sustracción, ocultación, destrucción e inutilización de medios de prueba. Esta figura prevé su modalidad imprudente en el segundo párrafo del art. 255 CP:

> "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)".

1.6. ¿Hay diferencias específicas entre la definición de los ciberdelitos y los delitos "tradicionales"?

No existe distinción en nuestra legislación. Más allá de haberse producido la reforma legislativa en forma asistemática y mediante normas no con-

temporáneas, mediando una suerte de diáspora de tipos penales en leyes especiales y en el Código Penal, al producir una actualización integral del último por la ley 26.388, no se marcaron diferencias.

2 | Técnica legislativa

2.1. ¿Hay problemas específicos respecto del principio de legalidad (p. ej., vaguedad, remisiones abiertas por parte del tipo penal a otras normativas)?

En general, los tipos penales resultan sumamente respetuosos del principio de legalidad. Es más, para evitar la constante remisión a otras normas se ha introducido, a través del art. 77 CP, un glosario de terminología.

2.2. ¿Cómo evita la legislación los efectos *chilling* indebidos sobre el uso legítimo de las TIC o de Internet?

No se advierten medidas expresas en la legislación vigente dirigidas a evitar que las tipicidades asumidas pudieran tener alguna derivación negativa, inhibitoria o restrictiva sobre los usos legítimos de las TIC o de Internet.

2.3. ¿Cómo evita la legislación penal el peligro de convertirse en obsoleta a la vista de la rápida innovación tecnológica?

2.3.1. Respecto de los cambios en el uso de Internet y de las redes sociales

En particular, el uso de Internet y de las redes sociales, como así también de gran parte de dispositivos móviles, no modifica las conductas típicas. A lo sumo, son nuevas herramientas para realizar las acciones ya contempladas en los tipos penales previstos por la reforma.

En algún caso, como la regulación del SCM por la ley 25.891, se incorporó en los tipos penales, como el art. 12, una fórmula como la siguiente: "o la tecnología que en el futuro la reemplace".

2.3.2. Respecto del progreso tecnológico (p. ej., mediante la remisión a las normas administrativas)

A través de muy paulatinas reformas al Código Penal de la Nación. O mediante modificaciones en algunas de las numerosísimas leyes especiales penales vigentes (alrededor de 70, al presente), por lo que la nota distintiva sería la de

falta de sistema, armonía y coherencia, aun cuando esto no sería particular de los delitos vinculados a las TIC, sino del ordenamiento punitivo nacional.

3 | Alcance de la incriminación

3.1. ¿En qué medida la legislación penal alcanza a meros actos preparatorios que conllevan un riesgo de abuso ulterior (p. ej., adquisición o tenencia de *software* que puede ser empleado para *hacking*, *phishing*, fraude de computadoras o elusión de las barreras de protección)?

Nuestra legislación pena la mera intrusión informática o acceso ilegítimo a un sistema informático (art. 153 *bis* CP).

3.2. ¿Se han suscitado controversias a partir de tal legistación?, ¿se han hecho esfuerzos legislativos específicos para prevenir la sobrecriminalización?

No hubo mayores controversias públicas, habiéndose ceñido la discusión a ámbitos académicos reducidos y sin mayor impacto externo. Los esfuerzos legislativos con vistas a adaptar la normativa de las nuevas modalidades de ataque a los viejos bienes jurídicos protegidos, ha sido tardía y se ha llevado a cabo luego de un largo reclamo de solución a problemas verificados jurisprudencialmente, como los de lagunas de punición.

3.3. ¿En qué medida la mera posesión o tenencia de ciertos datos resulta incriminada? ¿En qué áreas y con base en qué fundamentos? ¿Cómo se define la posesión o tenencia de datos? ¿Incluye la definición la posesión temporal o el mero visionado?

La posesión de datos personales resulta criminalizada. El elenco de figuras típicas vigentes no pune la mera posesión o tenencia de datos, sino otras conductas vinculadas, como por ej., el acceder a ellos, destruirlos, modificarlos con posible perjuicio, o difundirlos públicamente (siendo privados) o facilitar su acceso a no autorizados.

3.4. En la medida en que la posesión o el favorecimiento del acceso a ciertos datos hayan sido definidas como infracciones penales, ¿la responsabilidad penal se extiende a los proveedores de servicios (p. ej., proveedores de acceso o alojamiento)? ¿Cuáles son las exigencias para su responsabilidad, especialmente en lo que se refiere al tipo subjetivo

(*mens rea*)? ¿Están los proveedores obligados al seguimiento y control de la información que suministran o para la que ofrecen acceso, a dar información sobre la identidad de los usuarios, a impedir el acceso a ciertas informaciones? En caso afirmativo, ¿en qué condiciones y a qué costo? La violación de esas obligaciones, ¿puede generar responsabilidad penal?

La responsabilidad penal de los proveedores se rige por las reglas generales de la participación criminal. No hay normas particulares con relación a ellos en el ámbito penal. Sí existen numerosas previsiones administrativas, incluyendo aquéllas de orden sancionatorio, vinculadas al ejercicio de su rol dentro del sistema de comunicaciones.

3.5. ¿Qué limitaciones generales y, en particular constitucionales, han sido objeto de debate al incriminar conductas relativas a los crímenes concernientes a las TIC y a Internet (p. ej., libertad de expresión, libertad de prensa, libertad de asociación, intimidad, "principio de ofensividad", exigencia de un acto, no mera responsabilidad por resultado (exigencia de *mens rea*)?

Las principales objeciones han resultado como consecuencia de la posible afectación a la libertad de expresión y prensa.

En menor nivel, medió preocupación por posibles afectaciones a la intimidad (así, Corte Suprema Justicia Nación, en el caso "Halabi", al declarar inconstitucional la ley 25.873 en cuanto preveía la preservación por diez años de los datos de tráfico).

3.6. ¿Prevé la ley sanciones penales específicamente dirigidas a los ciberdelincuentes (p. ej., inhabilitación o suspensión temporal del uso de Internet)?

No existe una legislación que distinga tipos de autores y en función de ellos penas específicas.

4 | Alternativas a la criminalización

4.1. ¿Qué papel juega el derecho penal en relación a otras formas de combate del abuso de TIC y de Internet? ¿Qué relación existe entre las sanciones civiles y administrativas (pago de los daños, cierre de la empresa, etc.) y las sanciones penales en el área de las TIC?

Ninguno específico distinto a cualquier otro campo de la criminalidad.

4.2. ¿Qué medios no penales de combate contra las *websites* ofensivas se usan/difunden (p. ej., cierre de las *websites*, bloqueo del acceso a las websites)?

Ninguno.

4.3. ¿En qué medida se espera que los usuarios de las TIC apliquen medidas de autoprotección (p. ej., encriptación de mensajes, uso de *passwords*, uso de software de protección)? ¿Se prevén sanciones para la no protección del propio ordenador hasta cierto punto, p. ej., usando software antivirus o protegiendo con *password* el acceso a redes privadas? ¿La ausencia de razonable autoprotección supone un medio de defensa de los acusados por entrada ilícita o por abuso ilícito de la red de otra persona o de sus datos?

No existen hasta el momento campañas de autoprotección públicas en las cuales se concientice a los usuarios sobre el uso de programas de encriptación o protección de datos.

5 | Límites al anonimato

5.1. ¿Hay leyes o reglamentos que obliguen a los proveedores de Internet a almacenar los datos personales de los usuarios, incluyendo el historial del uso de Internet? ¿Pueden los proveedores ser obligados a suministrar esos datos a la policía?

Por el contrario, a partir de la sentencia de la CSJN en el caso "Halabi, Ernesto" se declaró la inconstitucionalidad del almacenamiento de información personal por parte de los proveedores de Internet.

Se hizo hincapié en que el problema era la previsión excesiva, de 10 años, cuando en derecho comparado es de 1 o 2 años.

5.2. ¿Obligan las leyes o reglamentos a los suministradores de servicios de Internet al registro de los usuarios con carácter previo al suministro de los servicios?

No se encuentra previsto en forma legal. Sin embargo, existen una gran cantidad de resoluciones administrativas y de reglamentaciones que regulan la prestación de servicios de Internet.

5.3. ¿Limitan las leyes o reglamentos las posibilidades de encriptación de archivos o mensajes en Internet? ¿Pueden los sospechosos ser obligados a *disclose* los *passwords* que usan?

La República Argentina no posee una figura específica que sancione la encriptación de archivos como ocurre en los Estados Unidos de América o Gran Bretaña e Irlanda del Norte. La mera encriptación de archivos no es delito en la República Argentina. Por el contrario, es una eficiente medida de autoprotección de datos personales.

6 | Internacionalización

6.1. ¿Se aplica la legislación doméstica a los datos ingresados en Internet desde el extranjero? ¿Hay una exigencia de "doble incriminación" para el ingreso de datos desde el extranjero?

6.2. ¿En qué medida el derecho penal de su país en el área de las TIC y de Internet se ha visto influido por los instrumentos jurídicos internacionales?

La ley 26.388 también ha seguido los lineamientos establecidos por el "Convenio sobre la Ciberdelincuencia de Budapest" del 23 de noviembre de 2001.(10)

En este sentido ha incorporado definiciones terminológicas en el art. 77 CP, teniendo en consideración las definiciones suministradas por el "Convenio sobre la Ciberdelincuencia de Budapest", en su art. 1, destinado a "Definiciones", perteneciente al Capítulo I, dedicado a la "Terminología".

En particular, también ha tenido presente este instrumento internacional para la redacción y descripción de la conducta típica del delito de ofrecimiento y distribución de imágenes relacionadas con pornografía infantil y tenencia de imágenes con fines de distribución (art. 128 CP), incorporando los verbos típicos establecidos su art. 9. En general, en lo referente a la modificación de los tipos penales alcanzados por la

(10) Ver Convenio sobre la Ciberdelincuencia, Budapest, 23/11/ 2001, Serie de Tratados Europeos nº 185, *Council of Europe / Conseil de L´Europe*.

ley 26.388, ha tomado en consideración el Capítulo II "Medidas que deberán adoptarse a nivel nacional", Sección 1, "Derecho penal sustantivo", para delimitar qué figuras penales indefectiblemente debían ser abarcadas por la reforma.

6.3. ¿Participa su país en debates sobre la armonización de la legislación relativa a los ciberdelitos (como el grupo de expertos intergubernamentales de las NN.UU sobre cibercrimen)?

Puntualmente, la Argentina participa de debates de armonización de su legislación en el MERCOSUR y UNASUR.

7 | Desarrollos futuros

7.1. Indique, por favor, las líneas actuales del debate jurídico y legislativo en su país concerniente a los delitos de Internet y relativos a la TIC.

En la actualidad, a través de la ley 26.685 se prevé la implementación gradual del expediente digital, firma, notificación y constitución de domicilios electrónicos. De igual forma, la CSJN, por medio de su Acordada 31/11 estipula la introducción gradual de la notificación electrónica.

Se ha presentado un proyecto[11] para tipificar en el CP la figura del robo de identidad digital, insertándola como art. 138 *bis* con la siguiente redacción:

> "Será reprimido con prisión de seis meses a tres años o multa de pesos veinte mil a pesos doscientos mil, el que sin consentimiento, adquiriere, tuviere en su posesión, transfiriere, creare o utilizare la identidad de una persona física o jurídica que no le pertenezca a través de Internet o cualquier otro medio electrónico, y con la intención de dañar, extorsionar, defraudar, injuriar o amenazar a otra persona u obtener beneficio para sí o para terceros".

(11) Por los senadores Marías de los Ángeles Higonet y Carlos Verna. Fuente: "Diario Judicial" del 28/05/2012.

También son objeto de debate la posible incriminación de conductas tales como: 1) La ciberocupación o registro impropio de nombres de dominio;[12] 2) El Spamming o correo basura o publicidad no solicitada;[13] 3) La captación ilegal y difusión de datos, imágenes y sonidos;[14] 4) La posesión simple de material pornográfico infantil; 5) La responsabilidad de los proveedores.[15]

(12) Ver Riquert Marcelo A., *Delincuencia Informática en Argentina y el Mercosur*, Prólogo de David Baigún, Bs. As., Ediar, 2009, pp. 202/204.

(13) Ver Riquert Marcelo A., *ibid.*, pp. 204/206.

(14) Ver Palazzi Pablo A., *"Los Delitos Informáticos en el Código Penal. Análisis de la ley 26.388"*, Bs. As., Editorial Abeledo Perrot, Bs. As., 2009, pp. 159/166, quien se inclina por su no punición y su amparo a través del derecho civil. También ver Riquert Marcelo A., *Delincuencia Informática en Argentina y el Mercosur*, *ibid.*, pp. 206/207, quien considera prudente y acertado postergar su punición hasta que exista un serio debate en torno a esta figura penal.

(15) Ver Tomeo, Fernando, "Responsabilidad penal de los administradores de sitios Web. El caso Taringa!", en *La Ley,* Bs. As., 1 de junio de 2011. También se sugiere ver Granero, Horacio R., "La naturaleza jurídica de la nube ('cloud computing')", en el *elDial.com,* Suplemento de Alta Tecnología, 09/09/2009, elDial.com DC11A9; Velazco San Martín Cristo, "Aspectos jurisdiccionales de la computación de la nube", en el *elDial.com,* Suplemento de Alta Tecnología Suplemento de Alta Tecnología, 14/04/2010, elDial.com DC1304; Elizalde, Marín Francisco, "La prueba en la Cloud Computing: Cloud Computing & Service Level Agreements. El modelo en los Estados Unidos de América y su proyección al ámbito local argentino", en el *elDial.com,* Suplemento de Alta Tecnología, 08/06/2011, elDial.com DC15EE; Teijeiro, Nicolás, "La protección constitucional de la intimidad en Internet con especial referencia a redes sociales", en el *elDial.com,* Suplemento de Alta Tecnología, 08/06/2011, DC15EF.

Sección 2

Relator General: **EMILIO VIANO**[1]

Grupo Nacional Argentino: **JAVIER AUGUSTO DE LUCA, MARCELO RIQUERT, CHRISTIÁN C. SUEIRO, MARÍA ÁNGELES RAMOS** y **FRANCISCO FIGUEROA**

1 | Prácticas legislativas y conceptos jurídicos

1.1. ¿Cómo se encuentran reguladas las normas penales relativas a los ciberdelitos en su país? ¿Se recogen en un título unificado o Código o se encuentran en códigos o títulos diversos? Aportar, por favor, las referencias adecuadas

Partiendo de un análisis político–criminal de la ley 26.388 de reforma en materia de criminalidad informática del Código Penal de la República Argentina —en adelante, CP—, puede verificarse en primer orden que, desde una perspectiva de la técnica legislativa empleada, el legislador ha acudido a la instrumentación de una ley de reforma integral, armónica y concordada al Código Penal de la Nación.

Sin embargo, desde que sancionó la primera ley con disposiciones penales con referencias directas a expresiones de las TIC (ley 24.766, BO 30/12/1996), se fueron sucediendo hasta 2008 una serie de reformas en leyes especiales o en el propio Código, que en forma parcial fueron incorporando tipos penales que responderían a lo que se identifica en el cuestionario como ciberdelitos. Por eso, existen previsiones fuera y dentro del Código. Entre

(1) Por dudas y consultas dirigirse al Relator General Profesor Dr. Emilio C. Viano: emilio.viano@gmail.com

las primeras, cuentan en particular las relativas a la propiedad intelectual, los delitos contra la hacienda pública o el sistema de seguridad social y los servicios de comunicaciones móviles.

1.2. ¿Cuál es el impacto de las decisiones judiciales en la formulación del derecho penal relativa a los ciberdelitos?

La ley 26.388 fue sancionada en 2008, con lo cual la jurisprudencia en materia de delitos informáticos resulta sumamente escasa hasta la fecha.

No obstante, decisiones judiciales que pusieron de manifiesto problemas de tipicidad (caso "Pinamonti" de 1991 para el daño informático y el caso "Autodesk" de 1997 para la propiedad intelectual) operaron de disparador para la adopción de reformas legislativas con mayor o menor celeridad.

1.3. Para hacer frente a las necesidades y circunstancias cambiantes y para alcanzar nuevos objetivos, algunas leyes sufren frecuentes reformas. Normalmente, tales reformas adoptan la forma de nuevas leyes. En algunos casos esas nuevas leyes, en lugar de modificar simplemente las partes de la ley que precisan ser cambiadas, incluyen las reformas requeridas en un texto consolidado junto con las anteriores modificaciones. Esta técnica se llama "refundición" (*recasting*). ¿Es así como las leyes sobre ciberdelitos son actualizadas y adaptadas a las realidades cambiantes en su país? Aportar, por favor, las referencias y citas adecuadas

En general, las reformas en materia penal en el área de cibercriminalidad resultan muy escasas y distanciadas en el tiempo. En su mayoría, han sido incorporadas al Código Penal para dotarlas de sistematicidad con las disposiciones de delitos tradicionales.

2 | Las infracciones específicas en materia de ciberdelitos

2.1. ¿En lo relativo a la *mens rea*, deben las infracciones en materia de ciberdelitos ser dolosas? ¿Se requiere un dolo específico?

La reforma de la ley 26.388 al CP se ha caracterizado por abarcar la modificación en su mayoría tipos penales dolosos, sin el empleo de tipos penales culposos a excepción del delito de "alteración, sustracción, ocultación, destrucción e inutilización de medios de prueba" (art. 255 CP), con

lo cual respeta la tradición jurídico-normativa de nuestra legislación penal en cuanto a mantener a los tipos culposos como *numerus clausus*.

En el mismo orden de ideas, la ley 26.388 no ha incorporado ningún tipo omisivo, ni doloso, ni culposo, lo cual evita ampliaciones del ámbito de punibilidad.(2)

En referencia a la existencia de un dolo específico, la reforma no ha incorporado en ninguna figura el empleo de un dolo específico o ultra-intención.

2.2. ¿Hay también delitos imprudentes en este ámbito? En caso afirmativo, por favor, aportar una lista de tales delitos

La legislación argentina prevé como tipo culposo o imprudente el tipo de alteración, sustracción, ocultación, destrucción e inutilización de medios de prueba:

> Art. 255 CP.- "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, este será reprimido con multa de pesos setecientos cincuenta ($ 750) a pesos doce mil quinientos ($ 12.500)".

3 | Integridad y funcionalidad del sistema TI

3.1. ¿Regula su derecho penal el acceso ilegal e interceptación de una transmisión?

La interceptación de comunicaciones está prevista en el artículo 197 CP.

(2) Ver Fillia, Leonardo César; Monteleone, Romina; Nager, Horacio Santiago; Rosende, Eduardo E. y Sueiro, Carlos Christian, "Análisis a la reforma en materia de criminalidad informática al Código Penal de la Nación (ley 26.388)", en *Suplemento de Derecho Penal y Procesal Penal,* La Ley, 28/08/2008, pp. 15/41.

3.2. Respecto del objeto (¿sistema o datos?), ¿califica su derecho penal como infracción penal la obstaculización grave, ilegítima, del funcionamiento de un ordenador y/o sistema electrónico, mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de información o datos de un programa, *software* o sistema informático?

Lo hace a través del tipo de daño del art. 183 CP.

Se prevé la alteración dolosa de registros fiscales (art. 12, ley 24.769) y la alteración de controladores fiscales (art. 12 *bis*, misma ley).

3.3. ¿Es un requisito de su derecho penal que el *hacker* lleve a cabo su conducta de acceso del sistema informático usando uno o más *software* necesarios para saltar las medidas de seguridad y lograr nivel de entrada o un nivel más elevado de acceso?

No es necesario, basta con el mero acceso.

4 | Interferencias con datos y sistemas

4.1. Respecto del objeto (¿protección del sistema/*hardware*/datos?), ¿define su derecho penal el concepto de "datos electrónicos y/o informáticos"? ¿Incluye esta definición los programas, el *software* o codificaciones similares? Si tiene una definición, apórtela por favor, así como la referencia a los correspondientes artículos/párrafos de su Código

La reforma 26.388 contempló específicamente la introducción de terminología al Código Penal de la Nación.

En particular, a través de la reforma al artículo 77 CP se incorporan los términos, documentos, firma, suscripción, instrumento privado en su modalidad digital.

Así, en el mencionado artículo 77 se incorporaron los siguientes párrafos:

> "El término 'documento' comprende toda representación de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión.
>
> Los términos 'firma' y 'suscripción' comprenden la firma digital, la creación de una firma digital o firmar digitalmente.
>
> Los términos 'instrumento privado' y 'certificado' comprenden el documento digital firmado digitalmente".

4.2. Respecto del acto, ¿qué penaliza su derecho penal: la destrucción, la alteración, el hacer inaccesible?

El art. 183 CP castiga a quien "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".

4.2.1. ¿Penaliza su derecho penal el borrado, alteración, conversión en inaccesible, adquisición u otra interferencia similar no autorizada con información o datos de un sistema o programa informático o electrónico?

Sí, específicamente a través de la afectación de bienes intangibles contemplados en el tipo penal de daño simple y agravado (arts. 183 y 184 CP).

4.2.2. ¿Penaliza su derecho penal la interceptación no autorizada de cualquier forma o modo de transmisión de información o datos informáticos o electrónicos?

Sí, a través de los tipos penales de violación de secretos y privacidad.

5 | Falsificación de datos

5.1. Respecto del objeto (¿la autenticidad?), ¿define su derecho penal como una infracción penal la introducción, alteración, borrado o supresión no autorizados de datos electrónicos o informáticos que produzca la inautenticidad de los datos con el fin de proteger la autenticidad de los datos susceptible de ser usados o aportados con fines jurídicos? Por favor, si dispone de una definición, apórtela junto a la referencia a los correspondientes artículos/párrafos de su Código y/o legislación especial

El art. 157 *bis*, inc. 3°, CP castiga la conducta de quien "ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales".

5.2. Respecto del acto (¿alteración/borrado?), ¿considera su derecho penal como infracción penal la introducción, alteración, borrado o supresión no autorizadas de datos/información electrónica o informática que produzca la inautenticidad de los datos/información con el fin de que sea considerados o aportados a efectos jurídicos como si fueran auténticos? En caso afirmativo, aporte, por favor, la referencia a los artículos/párrafos correspondientes de su Código

Sí, específicamente a través de la afectación de bienes intangibles contemplados en el tipo penal de daño simple y agravado (arts. 183 y 184 CP).

6 | Uso abusivo de dispositivos

6.1. Respecto del objeto (¿el tipo de dispositivos?), ¿penaliza su derecho penal el desarrollo de un "kit de herramientas" de hacker en todo o en parte (*por ejemplo* capturadores de contraseñas —*password grabbers*— y gestores de registro de claves —*key loggers*—, programas para realización de llamadas gratuitas —*blue boxing programs*—, programas de llamadas automáticas para encontrar vías de acceso a ordenadores y/o Internet —*war dialers*—, software de encriptado —*encryption software*—, programas de descifrado de contraseñas —*program password crackers*—, escáneres de vulnerabilidades de seguridad —*security vulnerability scanners*—, rastreadores de paquetes —*packet sniffers*— *etc.)* para el acceso no autorizado a sistemas o transmisiones electrónicas o informáticas?

No penaliza el desarrollo de herramientas, aplicaciones, ni programas, pero sí su empleo mediante la captación de datos personales.

6.2. Respecto del acto, ¿qué penaliza suy derecho penal: ¿la distribución,transferencia pública a otra persona?

6.2.1. ¿Penaliza su derecho penal el uso no autorizado de cualquiera de las herramientas de hacker recogidas en la pregunta 6.1.?

Penaliza el acceso a la información sin importar la herramienta empleada.

6.2.2. ¿Penaliza su derecho penal la distribución pública y/o transferencia a otras partes de la información electrónica hackeada?

Sí, mediante los tipos penales de: publicación abusiva de correspondencia (art. 155 CP), revelación de secretos (art. 157 CP), delitos relacionados con la protección de datos personales (art. 157 *bis* CP).

6.3. Respecto de la posesión, ¿penaliza su derecho penal la posesión de un "kit de herramientas" de hacker en todo o en parte (*por ejemplo* capturadores de contraseñas —*password grabbers*— y gestores de registro de claves —*key loggers*—, programas para realización de llamadas gratuitas —*blue boxing programs*—, programas de llamadas automáticas para encontrar vías de acceso a ordenadores y/o Internet —*war dialers*—, software de encriptado —*encryption software*—, programas de descifrado de contraseñas —*program password crackers*—, escáneres de vulnerabilidades de seguridad —*security vulnerability scanners*—, rastreadores de paquetes —*packet sniffers*— etc.) para el acceso no autorizado a transmisiones o sistemas electrónicos o informáticos?

Nuestro derecho penal no contiene una figura que reprima la tenencia de programas destinados al acceso ilegítimo.

7 | Intimidad. En torno a la violación del carácter secreto de datos privados

7.1. Objeto: ¿tipos de datos privados?(3)

7.1.1. ¿Requiere la legislación de su país que los recolectores de datos revelen sus prácticas de información con carácter previo a la recogida de información privada de los consumidores como, por ejemplo, qué información es usada, cómo se recoge y con qué fines, si se compartirá con otros o si los consumidores tendrán control sobre la revelación de sus datos privados?

7.1.2. Requiere la legislación de su país a las empresas y entidades que desarrollen sus negocios en Internet que informen a los consumidores sobre la identidad de quien recoge los datos, si el suministro de los datos requeridos es voluntario u obligatorio y los pasos dados por los colectores de los datos para asegurar la confidencialidad, la integridad y la calidad de los datos?

7.1.3. ¿Requiere la legislación de su país a las ***websites*** que publiquen su política de privacidad y expliquen cómo usarán la información personal antes de que los consumidores entren en el proceso de compra o en cualquier otra transacción para la que deban suministrar información sensible?

7.1.4. ¿Penaliza el derecho penal de su país el hecho de no suministrar las garantías relativas a la revelación mencionadas más arriba (7.1.1.; 7.1.2.; 7.1.3.)?

No existe un tipo penal específico que reprima la ausencia de garantías relativas a la protección de datos suministrados.

Puede haber regulación administrativa de algunos aspectos.

7.2. Acto: ¿uso y transferencia/distribución ilegal?

7.2.1. ¿Define el derecho penal de su país la transferencia y distribución ilegales de datos privados?

El art. 157 *bis* CP pune en su inc. 2° a quien "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) Datos privados son los datos que pertenecen a la vida privada de la gente pero que no identifican o hacen posible la identificación de una persona, por ejemplo, estado civil, orientación sexual, estado de salud, hábitos o preferencias de compra.

7.2.2. ¿Penaliza el derecho penal de su país el uso, transferencia y/o distribución ilegales de datos privados?

Sí.

7.3. Justificación

7.3.1. ¿En qué condiciones permite la legislación de su país la recogida, procesamiento, transferencia y distribución de datos privados?

Es tema regulado por la Ley de Protección de Datos Personales 25.326 (BO 02/11/2000), entendida por gran parte de la doctrina como reglamentaria de la garantía constitucional del art. 43 CN (*habeas data*).

7.3.2. ¿Qué nivel de necesidad se requiere para una recogida y/o distribución autorizadas (apremiante, importante, razonable, conveniente)?

8 | Intimidad. En torno a la violación de la confidencialidad profesional

8.1. Objeto: ¿tipo de datos privados?

8.1.1. ¿Requiere la legislación de su país que los profesionales revelen: (a) Sus prácticas de recogida y gestión de la información con anterioridad a la recogida de información personal de sus pacientes o clientes; (b) Sus prácticas de revelación; (c) Sus obligaciones éticas profesionales?

8.1.2. Si sus pacientes o clientes tienen control sobre la revelación de sus datos personales, ¿qué datos se encuentran, en su caso, protegidos de la manera específica?

8.1.3. ¿Autoriza o, incluso requiere, el derecho penal de su país al personal sanitario, abogados, sacerdotes, etc. violar la confidencialidad en ciertas situaciones o por ciertas razones legalmente establecidas? ¿En qué condiciones debería hacerse? (por ejemplo, causa razonable que permita ver o creer que hay abuso contra una víctima niño, mujer, persona de edad)?

Nuestra legislación no autoriza a los profesionales a revelar información confidencial, salvo en casos específicos (una epidemia), o por "justa causa", expresión cuyo contenido ha quedado reservado a la jurisprudencia. En algunos códigos procesales se menciona la obligación de denunciar los delitos contra la vida que determinados profesionales conozcan en el ejercicio de sus funciones, pero ello choca con otros principios como el deber de guardar el secreto profesional. La jurisprudencia se ha encargado de resolver cada caso de conflicto normativo.

8.2. Respecto del sujeto (¿tipo de autores?), ¿identifica el derecho penal de su país las categorías de profesionales sometidos a reglas de confidencialidad específicas?

8.3. Respecto del acto (¿uso y transferencia/distribución ilegales?), ¿qué actos (por ejemplo, *r*ecogida ilegal, uso, transferencia y distribución) son específicamente penalizados por la legislación penal de su país?

9 | Procesamiento ilegal de los datos personales y privados

9.1. Respecto del objeto, ¿penaliza su derecho penal la adquisición, procesamiento, almacenamiento, análisis, manipulación, uso, venta, transferencia, etc. no autorizados e ilegales de datos privados y personales?

9.2. Respecto del sujeto, ¿identifica su derecho penal de manera específica las categorías de personas y entidades incluidas en esta prohibición y sanciones penales?

9.3. Respecto del acto, ¿penaliza su derecho penal actos específicos que constituyen el todo o una parte del procesamiento ilegal de datos personales y privados? Responder, para cada categoría recogida a continuación, citando el derecho y disposiciones, en su caso, relevantes: (a) Recogida ilegal; (b) Uso ilícito; (c) Retención ilegal; (d) Transferencia ilícita

9.3.1. ¿Supone una diferencia el que esos datos personales y privados sean usados, transferidos etc. con fines policiales o de *law enforcement*?

9.4. Justificación

9.4.1. ¿En qué condiciones permite la legislación de su país la recogida, procesamiento, transferencia y distribución autorizados de datos personales y privados?

9.4.2. ¿Qué nivel de necesidad se requiere para la recogida y/o distribución autorizadas de datos privados y personales (apremiante, importante, razonable, conveniente)?

10 | Robo de identidad(4)

10.1. ¿Regula su derecho penal el robo de identidad?

Existe un proyecto de tipificación de robo de identidad de reciente trámite parlamentario, que propone un nuevo art. 138 *bis* al CP.

(4) El robo o usurpación de identidad se produce cuando alguien se apropia de la información personal de otro sin su conocimiento con el fin de cometer un delito de apropia

10.2. Objeto

10.2.1. ¿Penaliza su derecho penal el robo de identidad? Cite, por favor, el derecho relevante

No todavía.

10.2.2. ¿Proscribe su derecho penal formas específicas de robo de identidad como, por ejemplo, el *phishing*? Se considera el *phishing* como una forma de robo de identidad ***online*** que utiliza *emails* con identidad suplantada destinados para atraer a los receptores a *websites* fraudulentas que tratan de engañarlos para que divulguen datos financieros personales como los números de tarjetas de crédito, nombres de usuarios y passwords de cuentas, números de la seguridad social, etc.

No. Lo hace por vía indirecta a través de las figuras de generales de estafa y defraudación previstas en el art. 172 CP.

10.3. Respecto del sujeto, ¿conoce su derecho penal responsabilidad penal ligada a una personalidad digital de una persona o a su "avatar", o a su rol digital en un juego simulado por Internet (por ejemplo, *Cityville*, *Farmville*, etc.)? Cite, por favor, las fuentes jurídicas relevantes

No.

II | Protección contra contenido ilegal relacionado con las TIC. En torno a la pornografía infantil: ¿Imágenes de niños reales o virtuales?

11.1. ¿Penaliza su derecho penal el uso de Internet con objeto de almacenar, acceder y diseminar pornografía infantil? En caso afirmativo, citar las fuentes jurídicas relevantes

11.2. En particular, su derecho penal ¿crea un nuevo delito que apunta a los delincuentes que usan Internet para engañar y explotar niños con fines sexuales? En tal sentido, ¿convierte en delito en delito las siguientes acciones?

ción o de defraudación. El robo de identidad es un medio para la perpetración de esquemas de fraude. Típicamente, se lleva a la víctima a la creencia de que están divulgando información personal sensible para un negocio o entidad legítima, en ocasiones como respuesta a una solicitud por email de actualización de información de facturación o condición de miembro, o como solicitud para un puesto de trabajo o préstamo fraudulento por Internet.

11.2.1. Transmitir

Sí.

11.2.2. Hacer disponible

Sí.

11.2.3. Exportar

Sí.

11.2.4. Acceder Intencionalmente a pornografía infantil en Internet

Sí.

11.3. Su derecho penal, ¿permite a los jueces ordenar el borrado de la pornografía infantil colocada en sistemas informáticos en su país? ¿Permite que un juez ordene el embargo de todo material o equipo utilizado en la comisión de un delito de pornografía infantil?

El tipo penal de ofrecimiento y distribución de imágenes relacionadas con pornografía infantil se encuentra regulada en el art. 128 CP.

> Art. 128 CP.- "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 finales 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".

11.4. ¿Qué actos penaliza su derecho penal?

11.4.1. ¿Acceso a sabiendas a pornografía infantil por Internet?

Sí.

11.4.2. La transmisión de pornografía infantil por Internet

Sí

11.4.3. Exportar pornografía infantil en Internet

Sí.

11.4.4. Poseer pornografía infantil en Internet con el fin de transmitirla, exportarla

Sí.

11.4.5. La oferta online de niños con fines sexuales vía ***websites*** de redes sociales o chats

Sí.

11.5. ¿Es la definición de pornografía infantil de su Código Penal similar a la recogida en los instrumentos internacionales (Directivas UE)?

Sí.

11.6. ¿Se previene la victimización secundaria de las víctimas de pornografía infantil en su derecho penal? En Estados Unidos, país en el que la prostitución o la aparición en pornografía es un a acto castigado por el derecho penal nacional, debería ser posible la no persecución o no imposición de penas por ellas si el menor afectado ha cometido esos actos como resultado de su condición de víctima de explotación sexual o si el menor fue obligado a participar en la pornografía infantil. ¿Es esto lo que su derecho penal contempla?

No. En la Argentina no se reprime la prostitución ni la pornografía en sí mismas, sino su explotación cuando se trata de menores de edad o cuando existen medios violentos o fraudulentos en caso de mayores.

11.7. ¿Penaliza su derecho penal la pornografía "infantil virtual"?(5) Es decir, si la imagen no es la de un niño real, sino la resultante de una combinación de millones de pixeles informáticos realizada por un artista, ¿puede el gobierno de su país prohibir esta creación que, se alega, es sin víctimas? Citar, por favor, el derecho y/o decisiones judiciales aplicables

No se reprime, se requiere que se trate de menores reales. No puede tratarse de imágenes creadas por computadoras o fotomontajes.

(5) La pornografía "infantil virtual" no usa niños reales o imágenes de niños reales identificables.

11.8. Respecto del *mens rea*, para ser responsable, ¿la persona debería tanto tratar de entrar en un sitio donde la pornografía infantil se encuentra disponible como saber que esas imágenes pueden encontrarse ahí? En tal sentido, ¿su derecho penal establece que no deberían aplicarse penas a personas que, sin advertirlo, acceden a sitios que contienen pornografía infantil?

La acción descripta por el tipo penal es dolosa, con lo cual se requiere necesariamente que conozca y quiera acceder a un sitio de pornografía infantil para la aplicación de la figura.

12 | En torno a la incriminación que depende del uso de TIC

12.1. ¿Penaliza su derecho penal las conductas siguientes? Cite, por favor, el derecho relevante

12.1.1. Creación y uso de verdadero anonimato en el envío y/o recepción de material por las TIC

No se encuentra prevista ninguna figura.

12.1.2. ***Cyber-bullying***

Tampoco se encuentra contemplada una figura específica.

12.1.3. ***Cyber-stalking***

No posee una figura en particular.

12.1.4. ***Cyber-grooming***

Tampoco se contempla esta conducta como tipo penal específico.

12.2. Respecto del acto (creación/acceso/posesión/transferencia/distribución pública por las TIC), citar las leyes específicas que incriminan la creación (aun cuando no se use nunca), el acceso, la posesión (incluso si es solo privada), la transferencia y la distribución pública por Internet y otros medios electrónicos de otros materiales diferentes a los ya mencionados, especialmente debido al uso de la tecnología electrónica o de Internet

12.3. Respecto de las violaciones de la propiedad, incluida la propiedad intelectual, relacionadas con las TIC, ¿proscribe y penaliza específicamente su derecho penal las conductas siguientes perpetradas por medio del uso de las TIC? Citar, por favor, el derecho relevante

12.3.1. Defraudación

Sí, a través del tipo penal del art. 173, inc. 16 CP.

12.3.2. Infracción de los derechos de la propiedad intelectual

Sí, por medio de la ley 11.723.

12.3.3. Espionaje industrial

Sí, mediante todos los tipos penales transcriptos.

13 | Criminalización de actos cometidos en el mundo virtual

13.1. ¿Penaliza su derecho penal la comisión de delitos cometidos en el mundo virtual como, por ejemplo, pornografía infantil virtual, violencia virtual, grafitis virtuales, ciberdifamación, acoso sexual, acoso laboral, sin afectación de personas reales, solo mediante representaciones virtuales? Citar, por favor, el derecho relevante y aportar detalles

No contempla la existencia de tipos penales que repriman delitos virtuales.

14 | Delitos de *Non-compliance*

14.1. ¿Penaliza su derecho penal la no cooperación con las agencias policiales y/o de persecución en el campo del ciberdelito? Los deberes de cooperar pueden consistir en deberes de retener y almacenar información, producir/entregar información solicitada por una orden específica, dar acceso a los sistemas informáticos para la instalación de filtros o dispositivos, etc. En tal sentido, ¿es la infracción del deber de cooperar también susceptible de generar sanciones administrativas?
Citar el derecho relevante y aportar detalles

15 | Información complementaria opcional relativa a la práctica de aplicación de la ley (incluidas estadísticas)

15.1. ¿Se encuentran los ciberdelitos incluidos como tales en la recogida de datos sobre crimen en su país?

No.

15.2. ¿Hay una *website* en su país que suministre datos e información acerca de la frecuencia, gravedad, coste, impacto etc. de los ciberdelitos en su país?
En caso "afirmativo", aporte la dirección electrónica de la *website*

No que sea de nuestro conocimiento.

15.3. ¿Las encuestas de victimización de su país incluyen preguntas sobre ciberdelitos?

Generalmente, no.

15.4. ¿Qué tipos de delito informático/fraude informático son los más frecuentemente denunciados en su país?

15.5. ¿Tiene la policía y la fiscalía de su país una unidad de delitos informáticos? En caso afirmativo, ¿cuántos policías/fiscales las integran?

15.6. ¿Su Facultad u otra Facultad de su país ofrece cursos sobre ciberdelito? Aporte, por favor, la dirección de la web.

La Facultad de Derecho de la Universidad de Buenos Aires brinda dos cursos de ciberdelitos en la Carrera de Especialización de Derecho Penal.

La Facultad de Derecho de la Universidad Nacional de Mar del Plata, en su posgrado sobre "Criminalidad Económica" en conjunto con la Universidad Castilla La Mancha (España), tiene un módulo sobre "Delincuencia Informática".

La carrera de posgrado "Especialista en Derecho Penal Económico" de la Universidad Blas Pascal (Córdoba), tiene un módulo de "Delitos Informáticos".

15.7. ¿Es el tema del ciberdelito objeto de la formación inicial y/o continua de jueces, fiscales y policía?

No es objeto de capacitación obligatoria. Sin embargo, en la actualidad se están incrementando los cursos de capacitación y formación en materia de criminalidad informática.

15.8. Identifique, por favor, si las siguientes formas y medios de ciberdelincuencia: (a) ocurren con frecuencia, (b) ocurren de manera

infrecuente, o (c) no han tenido lugar en su país, colocando una "X" en la correspondiente casilla de la tabla siguiente:

Formas y medios de ciberdelincuencia	Ocurre frecuentemente	Ocurre infrecuentemente	No ha ocurrido
Robo de identidad *online* (incluido el *phishing* y el tráfico *online* de información sobre falsa identidad)			
Hacking (intrusión ilegal en sistemas informáticos)			
Código malicioso (gusanos, virus, *malware* y *spyware*)			
Interceptación ilegal de datos informáticos			
Comisión online de delitos contra la propiedad intelectual			
Tráfico *online* de pornografía infantil			
Daño intencional de datos o sistemas informáticos			
Otros			

Sección 3

Relator General: **JOHANNES F. NIJBOER**[1]

Grupo Nacional Argentino: **JAVIER AUGUSTO DE LUCA, MARCELO RIQUERT, CHRISTIÁN C. SUEIRO, MARÍA ÁNGELES RAMOS** y **FRANCISCO FIGUEROA**

I | Cuestiones Generales

1.1. ¿Existen definiciones (jurídicas o socio-jurídicas) para la aplicación de las TI y de las TIC en el contexto del procedimiento penal (incluida la práctica forense)? ¿Cómo están reflejadas estas definiciones conceptuales en la doctrina científica, la legislación, las decisiones judiciales y las prácticas pertinentes en el contexto del proceso penal?

Una de las principales dificultades que presenta la legislación argentina es que no se ha llevado a cabo una reforma procesal penal con respecto a la criminalidad informática que se adapte al "Convenio de Cibercriminalidad de Budapest".

Se encuentra pendiente la sanción de una ley procesal que regule la obtención, almacenamiento y conservación de prueba digital.

1.2. ¿Existen instituciones específicas y/o grupos de trabajo involucrados en la aplicación de las TIC en el sistema penal?

Sí, el Ministerio Público Fiscal tiene creada una comisión.

(1) Por dudas y consultas dirigirse al Relator General Profesor Dr. Johannes F. Nijboer: J.F.Nijboer@law.leidenuniv.nl

1.3. ¿Existen organizaciones (empresas) privadas (comerciales) que ofrecen servicios relacionados con las TIC en el sistema penal? Si es así, ¿puede dar ejemplos? ¿Qué límites tienen que ser observados?

No.

2 | Información e inteligencia: construyendo posiciones de información (*information positions*) para la aplicación de la ley

La construcción de posiciones de información es parte de la denominada actuación policial basada en la inteligencia. Se puede definir la actuación policial basada en la inteligencia como un marco conceptual para llevar a cabo la actividad policial como un proceso de organización de la información, actividad que se les permite a las agencias de aplicación de la ley en sus tareas preventivas y represivas.

2.1. ¿Qué técnicas relacionadas con las TIC utilizan las agencias de aplicación de la ley para la construcción de posiciones de información?

La principal técnica que se está empleando es la geolocalización de equipos celulares, mediante la activación remota de GPS o empleo de detección de antenas utilizadas por el dispositivo.

2.2. ¿A qué tipo de bases de datos públicas (por ejemplo, bases de datos de ADN) y privadas (por ejemplo, el Registro de Nombre de Pasajero o los datos financieros como los datos de SWIFT) tienen acceso las agencias de la aplicación de la ley?

Las agencias de aplicación de la ley tienen acceso a las bases de datos de la Administración Federal de Ingresos Públicos (AFIP), de la Administración Nacional de la Seguridad Social (ANSES), de la Dirección General de Aduanas (DGA), de la Dirección Nacional de Migraciones (DNM) y del Banco Central de la República Argentina (BCRA).

2.3. ¿Pueden aplicarse las técnicas consideradas como minería de datos y comparación de datos? Si es así, ¿pueden utilizarse estas técnicas para crear perfiles de posibles autores o grupos de riesgo? En tal sentido, ¿se han desarrollado herramientas especiales para las agencias de aplicación de la ley?

No se pueden aplicar las técnicas mencionadas.

2.4. ¿Pueden utilizarse medidas coercitivas (por ejemplo, la interceptación de las telecomunicaciones) para la construcción de posiciones de infomación?

Sí, bajo el régimen general reglado en los códigos procesales, mediante autorización judicial fundada.

La interceptación de telecomunicaciones móviles se encuentra prevista.

También existe el acceso a cuentas de correo electrónico, chat, o mensajería instantánea móvil, aunque no se haya implementado.

En particular, la mensajería instantánea móvil instalada en los celulares inteligentes (*Smarthphone*), presenta serias dificultades para su posible investigación por parte de agencias judiciales y policiales debido a que este tipo de mensajería instantánea (*BlackBerry Messenger, Whatsapp)*, se encuentra encriptada.

2.5. ¿Qué actores privados (por ejemplo, proveedores de Internet o empresas de telecomunicaciones) conservan o están obligados a conservar información para las agencias de aplicación de la ley?

Las empresas privadas no se encuentran obligadas por ley a la conservación de información y datos.

2.6. ¿Qué actores privados pueden proporcionar o están obligados a proporcionar información a las agencias de aplicación de la ley?

Ante el requerimiento judicial, proporcionan información los proveedores de Internet (Speedy, Fibertel), los servidores de correos electrónicos (Hotmail, Yahoo, Gmail), los motores de búsqueda (Google, Yahoo), las redes sociales (facebook, myspace, Hi5, Orkut, Sonico, etc.).

2.7. ¿Existe control judicial de la construcción de posiciones de información?

No existen hasta la fecha organismos especializados en la construcción de información digital.

3 | Las TIC en la investigación penal

3.1. ¿Pueden las agencias de aplicación de la ley llevar a cabo intervenciones en tiempo real de datos sobre el tráfico y sobre el contenido de los datos?

La ley 26.388 tuvo en consideración el "Convenio sobre la Ciberdelincuencia de Budapest" del 23 de noviembre de 2001. Sin embargo se limitó a

seguir sólo sus lineamientos parcialmente. Es decir, se adaptó nuestra legislación nacional únicamente respecto al derecho penal sustantivo, previsto en el Capítulo II "Medidas que deberán adoptarse a nivel nacional", Sección 1 "Derecho penal sustantivo", sin adaptar nuestra legislación a la Sección 2 de este instrumento internacional, dedicada al "Derecho Procesal".

Así que no se adoptaron medidas legislativas que permitan establecer procedimientos penales específicos para la obtención de prueba electrónica de cualquier delito cometido por medio de un sistema informático (art. 14 del Convenio sobre la Ciberdelincuencia de Budapest).

Tampoco se dio cumplimiento a la sanción de una legislación que prevea la "conservación rápida de datos informáticos almacenados", conforme lo requerido por el mencionado convenio en su Sección 2, Título 2.

Por tanto no existe una legislación nacional que prevea: 1) La conservación rápida de datos informáticos almacenados (art. 16 del Convenio sobre la Ciberdelincuencia de Budapest); 2) La conservación y revelación parcial rápida de los datos relativos al tráfico (art. 17 del Convenio sobre la Ciberdelincuencia de Budapest); 3) El orden de presentación (art. 18 del Convenio sobre la Ciberdelincuencia de Budapest); 4) El registro y confiscación de datos informáticos almacenados (art. 19 del Convenio sobre la Ciberdelincuencia de Budapest); 5) La obtención en tiempo real de datos relativos al tráfico (art. 20 del Convenio sobre la Ciberdelincuencia de Budapest); 6) Interceptación de datos relativos al contenido (art. 21 del Convenio sobre la Ciberdelincuencia de Budapest).

3.2. ¿Pueden las agencias de aplicación de la ley tener acceso/congelar/investigar/secuestrar los sistemas de información acerca de datos sobre el tráfico y del contenido de los datos?

El Poder Judicial de la Nación, por medio de la Corte Suprema de Justicia de la Nación, realizó profundas actualizaciones en materia de infraestructura tecnológica y capacitación del personal.[2] Sin embargo, en la actualidad no se cuenta con tribunales especializados en materia de criminalidad informática o área destinada específicamente a esta materia.

(2) Ver CSJN, "Justicia argentina online. La creación de la Agencia de Noticias del Poder Judicial" (*"Argentine Justicie online. The Creation of the News Agency of the Judiciary"*), Bs. As., Editorial Altura Impresores, 2010.

El Ministerio Público Fiscal (MPF), se encuentra en una situación análoga a la del Poder Judicial de la Nación, ya que si bien cuenta con un importante número de Unidades Fiscales temáticas o Unidades Especiales,[3] hasta la fecha no ha creado o destinado recursos para instaurar una Unidad Fiscal especializada en criminalidad informática, y se debe valer de los cuerpos periciales dependientes del Poder Judicial.

Idéntica realidad exhibe el Ministerio Público de la Defensa (MPD), que también posee una gran cantidad de comisiones y programas,[4] como así también un importante Departamento de Informática dentro del área de la Dirección General de Administración de la Defensoría General de la Nación, pero que hasta el presente no dispone de ninguna comisión o programa especializado en criminalidad informática.

En cuanto a los auxiliares de la Administración de Justicia, como la Policía Federal Argentina (PFA), la Gendarmería Nacional Argentina (GNA), la Prefectura Naval Argentina (PNA) y la Policía de Seguridad Aeroportuaria (PSA), solo los dos primeros cuentas con áreas especializadas de investigación.

3.3. ¿Se puede obligar a las empresas de telecomunicaciones o proveedores de servicios a compartir los datos con las agencias de aplicación de la ley? En caso de incumplimiento, ¿hay medidas coercitivas o sanciones?

Es una situación compleja, ya que la mayoría de las empresas (Google, Hotmail, Yahoo, Facebook, entre otras) son transnacionales y, por lo tanto, es difícil aplicarle medidas coercitivas o sanciones. Además, la mayoría de

(3) Entre sus Unidades Especiales pueden mencionarse: 1) U.F. AMIA (UFIA); 2) U.F. de asistencia en Secuestros Extorsivos y Trata de Personas (UFASE); 3) U.F. de investigación de Delitos de Tributarios y Contrabando (UFITCO); 4) U.F. para la investigación de Delitos relativos a la Seguridad Social (UFISS); 5) U.F. para los delitos cometidos en el ámbito del PAMI (UFIPAMI); 6) U.F. para los delitos cometidos en el ámbito del Registro Nacional de Armas (UFIRENAR); 7) U.F. para la investigación de Delitos contra la Integridad Sexual y Prostitución Infantil; 8) U.F. para la investigación de delitos contra el Medio Ambiente; 9) U.F. de investigación de Lavado de Dinero y Financiamiento del Terrorismo; 10) U.F. de coordinación de causas de violación de Derechos Humanos durante el Terrorismo de Estado; 11) U.F. para la investigación de violencia en Espectáculos Deportivos [en línea], http://www.mpf.gov.ar/index.asp?page=Organigrama/organigrama.html

(4) La Defensoría General de la Nación cuenta con los siguientes programas y comisiones: 1) Comisión de Cárceles; 2) Comisión de Seguimiento del Tratamiento Institucional de Niñas, Niños y Adolescentes; 3) Comisión para la Asistencia Integral y Protección al Refugiado y Peticionante de Refugio; 4) Comisión de Seguimiento del Tratamiento Institucional de Neuropsiquiátricos; 5) Comisión de Temática de Género; Comisión del Migrante; 6) Programa de Asistencia y Patrocinio Jurídico; 7) Programa para la Aplicación de Tratados

esas empresas se rigen por sus políticas de privacidad para determinar en qué casos brindar información.

3.4. ¿Pueden las agencias de aplicación de la ley realizar video vigilancia? ¿Pueden obligar a las personas físicas o jurídicas a cooperar?

La video vigilancia resulta una herramienta tecnológica permitida en espacios públicos, no así en espacios privados, ni en domicilios. No se encuentra autorizada la escucha acústica de domicilio o el empleo de cámaras térmicas.

Algunas leyes procesales penales provinciales (la Argentina es un país federal, dividido en provincias y cada una tiene su Código Procesal Penal) regulan entre los medios de prueba a las filmaciones de sistemas de monitoreo público o privado y a grabaciones de las llamadas a teléfonos del sistema de emergencias.

3.5. ¿Pueden o deben aplicar las agencias de aplicación de la ley la grabación audiovisual de los interrogatorios (sospechosos, testigos)?

Pueden realizarse grabaciones de juicios, audiencias orales antes las Cámaras de Apelaciones de los distintos fueros.

Hay previsiones específicas, como la filmación y grabación de declaraciones de víctimas menores de edad de abusos sexuales (Cámara Gesell), generalmente usadas como anticipo extraordinario de prueba con videofilmación u otro medio similar de registración del acto.

También para registrar audiencias orales en la etapa de la investigación penal preparatoria y de ejecución de la pena, en las que las resoluciones judiciales son oralizadas.

4 | Las TIC y la prueba

Etapas que atraviesa la prueba digital y/o electronica: recogida/almacenamiento/retención/producción/ presentación/valoración.

Internacionales de Derechos Humanos; 8) Programa de Atención a las Problemáticas Sociales y Relaciones con la Comunidad; 9) Programa Piloto para la Asistencia Jurídica a Mujeres Privadas de la Libertad [en línea], www.mpd.gov.ar

4.1. ¿Existen reglas sobre la prueba específicas para la información relacionada con las TIC?

Pese a existir modificaciones al Código Procesal Penal de la Nación, no se ha realizado una reforma procesal penal en materia de criminalidad informática. Se necesita orden judicial para los requerimientos e interceptaciones y se equipara el medio a los recaudos que deben tomarse cuando se trata de correspondencia y telecomunicaciones.

4.2. ¿Existen reglas sobre la integridad (por ejemplo, manipulación o procesamiento incorrecto) y seguridad (por ejemplo, *hacking)* de la prueba relativa a las TIC?

Ante la ausencia de ley procesal, no existen reglas de integridad o protocolos para la manipulación de prueba digital. Debe aclararse que en la Argentina rige el principio de libertad probatoria, de modo que para dotar a las pruebas de las pautas de seguridad necesarias (no contaminación, no pérdida de las cadenas de seguridad, inalterabilidad, etc.), se recurre a peritos oficiales, como con cualquier otra prueba.

4.3. ¿Existen reglas sobre la admisibilidad (incluido el principio de legalidad procesal) de las pruebas que son específicas de la información relacionada con las TIC?

No existen ese tipo de reglas.

4.4. ¿Existen reglas específicas sobre el descubrimiento y revelación de la prueba relacionada con las TIC?

No existen ese tipo de reglas específicas.

4.5. ¿Existen reglas especiales para la valoración (valor probatorio) de la prueba relacionada con las TIC?

No existen ese tipo de reglas específicas.

5 | Las TIC en la etapa de juicio

5.1. ¿Cómo puede o debe introducirse en el juicio la prueba relacionada con las TIC?

Deben ser introducidas a pedido de parte y con el control de ellas.

5.2. ¿Pueden realizarse interrogatorios a distancia (por ejemplo, conexiones vía satélite)?

Se han implementado los métodos de declaración testimonial a distancia.

5.3. ¿Pueden utilizarse técnicas digitales y virtuales para la reconstrucción de los hechos (asesinatos, accidentes de tráfico)?

Sin lugar a dudas, el empleo de mapas satélitales como Google maps o Google Earth, sistemas de coordenadas, GPS y programas y aplicaciones de geolocalización como "foursquare".

5.4. ¿Pueden utilizarse técnicas audiovisuales para presentar pruebas en el juicio (en su forma más simple: imágenes y sonido)?

Sí.

5.5. ¿Pueden sustituirse los expedientes penales en "papel" por otros electrónicos? ¿Se ha avanzado hacia la digitalización de los documentos del juicio?

Hasta la fecha no, gradualmente se producirá en la República Argentina a través de la ley 26.685, la transición al expediente digital y la gradual sustitución del expediente en soporte papel.

Un significativo avance por parte del Poder Judicial de la Nación de la República Argentina, es la labor encarada por la Corte Suprema de Justicia de la Nación, quien ha digitalizado todas sus sentencias y gran parte de su biblioteca. En igual sentido, ha comenzado con los cursos de capacitación para la implementación gradual de la Acordada 31/2011, tendiente a la constitución de domicilios electrónicos de notificación.

No debe perderse de vista que, en un país con estructura federal en el que los códigos procesales han quedado reservados a las provincias y, además, el Código Procesal Penal de la Nación es de los más antiguos en cuanto a su adscripción a un sistema mixto con rasgos inquisitivos, en el orden local puede haber previsiones más actuales, como las citadas de la provincia de Buenos Aires, donde hoy es común que actos centrales del proceso se documenten mediante registración de audio/video digitales con una breve acta escrita que complementa en el legajo tradicional, dejándose constancia del acto celebrado.

Sección 4

Relator General: **ANDRÉ KLIP**[1]

Grupo Nacional Argentino: **JAVIER AUGUSTO DE LUCA, MARCELO RIQUERT, CHRISTIÁN C. SUEIRO, MARÍA ÁNGELES RAMOS** y **FRANCISCO FIGUEROA**

I | Cuestiones sobre la jurisdicción

1.1. ¿Cómo localiza su país el lugar de comisión de un delito cometido en el ciberespacio?

En Argentina, en la mayoría de los casos, se determina el lugar de la comisión del delito a través de la dirección IP que utiliza el ordenador al conectarse a la red y mediante el cual se realiza el acto delictivo. En los casos en que la IP es enmascarada o adulterada, el lugar de comisión se determina a través del último lugar de donde hubo una conexión con el número de IP.

En Argentina, la aplicación de la ley penal está determinada en el art. 1 CP, donde se establece su aplicación a aquellos delitos cometidos en el territorio nacional, sus efectos se produzcan allí o en lugares sometidos a nuestra jurisdicción. Es decir, únicamente tendríamos jurisdicción para juzgar los delitos cometidos en Argentina o, aquellos, cuyos efectos se produzcan en nuestro país, aún en los casos en que la acción haya sido realizada fuera de nuestras fronteras.

(1) Por dudas y consultas, dirigirse al Relator General, Profesor Dr. André Klip: andre.klip@maastrichtuniversity.nl

1.2. ¿Su legislación nacional considera necesario y posible localizar el lugar donde se encuentran la información y las pruebas? ¿Dónde está la información que se puede encontrar en la web? ¿Se encuentra donde el ordenador del usuario está físicamente presente? ¿Allí donde el proveedor de la red tiene su sede (jurídica o de hecho)? ¿Qué proveedor? ¿O es el lugar de la persona que posibilitó la disponibilidad de los datos? Si estas preguntas no se consideran jurídicamente relevantes, por favor, indique por qué

En primer lugar, debemos poner de resalto que, por el momento, nuestro país carece de una ley de procedimientos en materia penal que contemple las situaciones planteadas.

No obstante, consideramos que resulta trascendental conocer dónde se almacena la información que puede llegar a ser prueba digital en un proceso penal.

Si bien, en la mayoría de los casos donde se considera que puede haber prueba digital se suelen secuestrar ordenadores y sus discos rígidos, lo cierto es que actualmente la evidencia ya no se guarda en esas fuentes de almacenamiento, sino que se suele guardar la información en "la nube" (*cloud computing*), el ciberespacio o servidores en el extranjero. Por tal razón es que entendemos que resulta necesario conocer dónde se almacena la información para proceder con la mayor celeridad del caso y evitar la pérdida de prueba relevante para el proceso penal.

En ese sentido, creemos que la computación en "la nube" (*cloud computing*), será uno de los temas sobre los que deberá versar la discusión legislativa en material procesal penal, para así lograr su introducción con las medidas de seguridad informática y, así, evitar almacenar información en servidores situados fuera del territorio nacional.

1.3. ¿En su sistema penal se puede prescindir de la determinación del *locus delicti* en caso de cometerse un ciberdelito? ¿Por qué?

En principio, cuando estamos frente a un ciberdelito propiamente dicho no se podría prescindir del *locus delicti*; sin embargo, sí se podría evitar en caso de encontrarnos ante un delito de jurisdicción universal cometido a través de la Internet o en el cual las pruebas fundamentales están en la Internet.

1.4. ¿Qué normas de competencia jurisdiccional se aplican a los ciberdelitos tales como la incitación al odio a través de Internet, *hacking*, ataques contra los sistemas informáticos, etc.? Si su Estado no tiene jurisdicción sobre estos delitos, ¿se considera es esto problemático?

Ante los casos planteados se aplicarían las normas generales ya descriptas.

1.5. ¿Su legislación nacional contiene normas relativas a la prevención o a la solución de los conflictos de jurisdicción? ¿Hay alguna práctica sobre ello?

La legislación nacional argentina no posee normas específicas relativas a la prevención o solución de conflictos de jurisdicción en materia de ciberdelitos. No obstantes, se aplican los principios generales de aplicación de la ley penal, es decir, el principio de territorialidad y extraterritorialidad; de extensión de la jurisdicción, tanto el real o de defensa, universal o personal.

1.6. ¿En su sistema penal se puede prescindir de los principios jurisdiccionales en caso de que se cometa un ciberdelito, lo que en esecia significa que el Derecho penal nacional es de aplicación universal? ¿Debería esto limitarse a ciertos delitos, o estar condicionado a la existencia de un tratado?

La legislación de la República Argentina no prevé que se pueda prescindir de los principios jurisdiccionales en ningún caso y, tampoco, contempló una regulación especial para la criminalidad informática.

2 | Derecho penal sustantivo y sanciones

2.1. ¿Qué ciberdelitos tipificados en su sistema penal nacional considera usted que tienen una dimensión transnacional?

Consideramos que unos de los delitos con mayor dimensión transnacional es el de ofrecer, almacenar y distribuir pornografía infantil (art. 128 CP).

Además, también consideramos relevantes, a raíz de la intangibilidad del software y del almacenamiento digital de información, los siguientes delitos: (a) Violación de correspondencia electrónica (art. 153 CP); (b) Acceso ilegítimo a un sistema informático (art. 153 *bis* CP); (c) Publicación abusiva de correspondencia (art. 155 CP); (d) Revelación de secretos (art. 157 CP); (e) Delitos relacionados con la protección de datos perso-

nales (art. 157 *bis* CP); (f) Defraudación informática (art. 173, inc. 16, CP); (g) Daños (arts. 183 y 184, CP); (h) Interrupción o entorpecimiento de las comunicaciones (art. 197 CP); (i) La alteración, sustracción, ocultación, destrucción e inutilización de medios de prueba (art. 255 CP).

2.2. ¿En qué medida las definiciones de los ciberdelitos contienen elementos jurisdiccionales?

La reforma que fue realizada en materia de criminalidad informática (ley 26.388) no introdujo en la descripción típica de las conductas ningún elemento que haga referencia a la jurisdicción.

2.3. ¿Hasta qué punto las reglas de la parte general sobre la comisión, conspiración o cualquier otra forma de participación contienen elementos jurisdiccionales?

La parte general de nuestro derecho penal se aplica a todos los delitos, sin embargo no contienen elementos jurisdiccionales en materia de ciberdelitos.

2.4. ¿Considera usted que los ciberdelitos constituyen un asunto que un Estado puede regular por sí mismo? Si es así, indique cómo puede hacerlo un Estado. Si no es así, indique por qué no puede hacerlo

Consideramos que los estados pueden (y deben) regular por sí mismo los ciberdelitos, sin embargo, para que ellos sea posible es indispensable que haya cooperación internacional y compatibilidad de legislaciones. Sobre todo en esta clase de delitos que tienen la particularidad de ser transnacionales a raíz de la fluidez de la información en Internet y el gran problema que presenta la aplicación de la ley penal en el espacio.

2.5. ¿Su derecho penal nacional prevé la responsabilidad penal de las empresas/proveedores (internacionales)? ¿Tiene la atribución de responsabilidad implicaciones jurisdiccionales?

En la actualidad y por el momento nuestra legislación penal no prevé la responsabilidad penal de las personas jurídicas en materia de criminalidad Informática.

3 | Cooperación en materia penal

3.1. ¿Hasta qué punto las especificidades de la tecnología de la información cambian la naturaleza de la asistencia mutua?

No debería cambiarlas desde una perspectiva teórica. En lo práctico, las asimetrías de disponibilidad tecnológica entre los Estados pueden obstar a una efectiva asistencia mutua.

3.2. ¿Se prevé en su país la interceptación de telecomunicaciones (inalámbricas)? ¿Bajo qué condiciones?

Sí, nuestra legislación prevé la interceptación de telecomunicaciones. Sin embargo, no puede ser ordenada por cualquier actor procesal, sino que únicamente puede hacerlo el juez mediante una resolución fundada.

3.2.1. ¿En qué medida es relevante que un proveedor o un satélite puedan estar ubicados fuera de las fronteras del país?

Consideramos que resulta relevante para poder someterlo a la jurisdicción nacional.

3.2.2. ¿Su legislación nacional prevé la asistencia judicial mutua en relación a la interceptación de las telecomunicaciones? ¿Ha celebrado su país convenios internacionales al respecto?

Históricamente la República Argentina participó de los tratados internacionales de cooperación en materia de adquisición y producción de pruebas. En el ámbito interno rige la Ley de Cooperación Internacional en Materia Penal (ley 24.767, BO 16/01/1997), cuyos principios generales podría ser aplicado en materia de interceptación de telecomunicaciones.

3.3. ¿En qué medida las causas generales de denegación se aplican en relación a las investigaciones en Internet y otros medios para acceder a los ordenadores y las redes ubicadas en otros lugares?

La medida es la misma que para cualquier acto de cooperación, ya que no hay previsión específica aún acerca de investigaciones en Internet.

3.4. ¿Se exige en su legislación nacional el requisito de la doble incriminación para la cooperación en aquellas situaciones en las que el autor haya causado los efectos desde un Estado en el que se permite la conducta en un Estado en el que se tipifica como delito la conducta?

Sí se exige, al igual que en los procesos de extradición.

3.5. ¿Permite su legislación nacional las investigaciones extraterritoriales? ¿Bajo qué condiciones? Por favor, responda tanto a la situación en la que las autoridades nacionales de aplicación de la ley necesitan información, como cuando las autoridades extranjeras necesitan la información disponible en su Estado

Toda investigación en el exterior, se rige por los principios generales de la cooperación internacional, tanto si nuestros magistrados y funcionarios se constituyen en el extranjero, como si las autoridades extranjeras se hacen presente en nuestro país. En cualquier caso, se necesita la aprobación de los magistrados del país requerido.

3.6. ¿Se permite el autoservicio (*self service*), es decir, la obtención de pruebas en otro Estado sin pedir permiso? ¿Qué condiciones deben cumplirse para permitir el autoservicio? Por favor, diferenciar la información pública y la protegida. ¿Cuál es la práctica (tanto activa como pasiva) en su país?

No se permite. En los casos que se trate de información privada se rige por las reglas del derecho internacional y los principios de libertad probatoria.

No existe legislación procesal penal específica sobre ese asunto en materia de cibercriminalidad.

3.7. Si es así, ¿se aplica esta legislación también a las búsquedas que se llevan a cabo en la *web* de acceso público, o en ordenadores que se encuentran fuera del país?

Sí, se puede hacer desde la Argentina. En ese caso, rige el principio de libertad probatoria, pero también el de defensa en juicio, que exige que la defensa haya tenido la posibilidad de controlar la prueba.

3.8. ¿Es su país parte en acuerdo sobre el Registro de Nombre de Pasajero (PNR) (transacciones financieras, intercambio de ADN, cuestiones de visados o similares)? Por favor, especificar y explicar cómo se lleva a cabo el intercambio de datos en la legislación nacional. ¿Tiene su país una llamada unidad que está disponible 24 horas al día y 7 días a la semana para el intercambio de datos? Limítese a las cuestiones relevantes sobre uso de la información para la investigación criminal

Hasta la fecha no se cuenta con una unidad especializada en el intercambio de datos.

3.9. ¿Hasta qué punto los datos a que se refiere en su respuesta a la pregunta anterior se intercambian para la investigación criminal y cuál es el fundamento jurídico? ¿Hasta qué punto la persona concernida tiene la posibilidad de impedir/corregir/eliminar la información? ¿En qué medida puede esta información ser utilizada como prueba? ¿La ley de su país permite la detección y retirada de un sitio web que contiene información ilegal? ¿Existe alguna práctica? ¿Desempeña algún papel el sitio del proveedor, propietario del sitio o cualquier otro elemento extranjero?

En la Constitución Nacional Argentina se prevé la acción de *hábeas data*, que es una herramienta de fácil y ágil acceso para el ciudadano a efectos de detectar, hacer corregir o retirar los datos personales que figuren en bases que pudieran ser no autorizados, excesivos o incorrectos.

3.10. ¿Cree usted que es posible un sistema de aplicación internacional para ejecutar las decisiones (por ejemplo, órdenes de suspensión de Internet o inhabilitaciones) en el área de la delincuencia cibernética?

Sí, conforme las recomendaciones realizadas por el Convenio de Ciber-criminalidad de Budapest.

3.11. ¿Su país permite la consulta directa de bases de datos nacionales o internacionales que contienen información relevante para las investigaciones criminales sin solicitud?

Si bien existen registros públicos a los que se pueden acceder sin solicitud, también existen otros registros a los que sólo se puede acceder con orden judicial.

3.12. ¿Participa su país en Interpol/Europol/Eurojust o cualquier otro organismo supranacional que aborde el intercambio de información? ¿Bajo qué condiciones?

En la actualidad la Argentina participa con Interpol y Europol.

4 | Aspectos relacionados con los derechos humanos

4.1. ¿Qué normas de derechos humanos o constitucionales son aplicables en el contexto de las investigaciones penales con tecnología de la información? ¿Es relevante para la determinación de las normas aplicables de derechos humanos el lugar en el que se consideraque se han realizado las investigaciones?

Todas las normas de derechos humanos o constitucionales se aplican en los procesos penales, sin embargo no hay ninguna específica sobre cibercriminalidad.

4.2. ¿Cómo se regula la responsabilidad o rendición de cuentas (*accountability*) de su Estado involucrado en la cooperación internacional? Por ejemplo, ¿es su Estado responsable del uso de la información recolectada por otro Estado en violación de las normas internacionales de derechos humanos?

No está regulado de manera específica.

5 | Desarrollos futuros

5.1. Las modernas telecomunicaciones ofrecen la posibilidad de contactar directamente con los acusados, víctimas y testigos a través de las fronteras. ¿Se debería permitir eso y, en caso afirmativo, en qué condiciones? Si no es así, ¿se deberían aplicar las reglas clásicas de asistencia mutua (solicitud y respuesta), y por qué?

En Argentina, en la actualidad, en varias causas penales se permite la videoconferencia para recibir prueba. Sin embargo, donde más se está utilizando esta modalidad es en las causas vinculadas a graves violaciones a los derechos humanos y de megacriminalidad, en las que se permitió que las videoconferencias se realicen con personas que se encuentran residiendo en el extranjero. Lo mismo ocurre con el envío de documentos

escaneados, cuando son certificados en el país de origen, por ejemplo, por nuestro consulado.

En ese sentido, creemos que es sumamente aconsejable y, por suerte, ya lo estamos implementando.

5.2. ¿Existe algún impedimento legal en su legislación para las audiencias a través de medios audiovisuales (a través de *Skype* o de otro medio) en casos transnacionales? Si es así, especificar cuál. Si no es así, especificar si hay alguna práctica

Si bien no existe ningún impedimento legal para utilizas esos medios audiovisuales, por el momento no se encuentra específicamente regulado, aunque cada vez se utiliza con mayor habitualidad.

5.3. ¿Hay alguna otra cuestión relacionada con la sociedad de la información y el derecho penal internacional que actualmente juega un papel en su país y no ha sido tratado en las preguntas anteriores?

La computación en "la nube" (*cloud computing*) y el almacenamiento de información en servidores que se encuentran fuera de la jurisdicción nacional, en particular cuando la información a resguardarse es información que puede provenir de los organismos públicos del Estado.

Proyectos de investigación

Una aproximación al trabajo de la Oficina de Intervención Interdisciplinaria en el abordaje de las personas privadas de libertad

Coordinado por **EQUIPO DE INTERVENCIÓN INTERDISCIPLINARIA**[1]

1 | Introducción

La Oficina de Intervención Interdisciplinaria (OII) —dependiente en la actualidad de la Secretaría General de Derechos Humanos— fue creada en el mes de julio de 2008, con la intención manifiesta de abrir un espacio en la Defensoría General de la Ciudad Autónoma de Buenos Aires para articular las diversas miradas que aportan distintas disciplinas —el trabajo social, la psicología y el derecho, entre otras— con el fin de aplicarlas a la atención de personas en situación de vulnerabilidad y/o riesgo social y que se encontraran en conflicto con la ley penal. En el presente artículo abordaremos las prácticas que el equipo de la OII realiza con personas privadas de libertad.

Cabe destacar que al proponerse un abordaje interdisciplinario se apuesta a lograr una comprensión más rica, más compleja, de una problemática

(1) Integrado por: Javier Scipioni (abogado y psicólogo, Jefe de la Oficina de Intervención Interdisciplinaria); Eloísa Moira Salas (abogada); Héctor Borguez Tosar (abogado); Valeria Vegh Weis (abogada); Miguel Orellano (psicólogo); Carolina Raggio (trabajadora social); Yael Barrera (trabajadora social); Luis Fresia (psicólogo); Tamara Rotundo (psicóloga); Yanil Amato (trabajadora social); Agustina Ciccola (politóloga); Sabrina Scocco (estudiante de Trabajo Social); Fernando Rodríguez Zuñiga (administrativo); Pablo Tsipkis (administrativo).

determinada por múltiples factores, dando lugar, a partir de ella, a la planificación de acciones que tiendan a incidir favorablemente sobre la situación concreta que padece la persona asistida.

En definitiva, se trata de forjar un espacio donde los distintos saberes se reúnan y dialoguen para lograr una síntesis superadora. En este sentido, el abordaje de los casos se realiza en el marco de un equipo que se reúne periódicamente.

Se confeccionan actas para asegurar la continuidad en el trabajo como así también protocolos de actuación para garantizar estándares de intervención. También hay distribución de funciones entre los miembros del equipo, conformándose, cuando se estima conveniente, grupos de trabajo específicos.

2 | Presupuestos teóricos de nuestra intervención

Nuestro enfoque teórico parte de concebir a la selectividad penal como una de las características estructurales del poder punitivo.[2] Se trata de una selectividad clasista, de género, étnica y religiosa, que dirige el poder punitivo hacia sujetos con alta vulnerabilidad social, identificados por las fuerzas de seguridad en base a estereotipos conformados en función de prejuicios éticos y estéticos (siguiendo la pauta de asociar lo feo a lo malo, tan cara al positivismo).

La selectividad opera particularmente en dos estratos. Por un lado, en la denominada "criminalización primaria": el poder legislativo sanciona un programa legislativo en materia penal que hace hincapié en los delitos contra la propiedad, por sobre el conjunto de las conductas disvaliosas. Por otro lado, se impone la "criminalización secundaria" en la que las agencias policiales aplican este programa punitivo en un doble recorte

(2) Bergalli, Roberto, *Control social punitivo. Sistema penal e instancias e aplicación (Policía, Jurisdicción y Cárcel)*, Barcelona, M. J. Bosch, 1996; Ferrajoli, Luigi, *Derecho y Razón*, Madrid, Trotta, 2001; Pavarini, Màssimo, *Control y Dominación. Teorías criminológicas burguesas y proyecto hegemónico*, Siglo XXI, Bs. As., 2003; Zaffaroni, E. Raúl, *Política Criminal Latinoamericana; Perspectivas-disyuntivas*, Bs. As., Hammurabi, 1982.

selectivo: se aplican solo algunos tipos penales —los que condensan los delitos más burdos, de más fácil persecución y recolección de prueba— y sobre determinados sectores de la población en particular en base a un estereotipo criminal estigmatizante: "los pibes chorros".

Una clara consecuencia de la criminalización secundaria es que:

> "en el imaginario público las prisiones se hallen pobladas por autores de hechos graves, como homicidios, violaciones, etc. (los llamados delitos naturales) cuando en realidad la gran mayoría de los prisionalizados lo son por delitos groseros cometidos con fin lucrativo (delitos burdos contra la propiedad y tráfico minorista de tóxicos, es decir operas toscas de la criminalidad)".(3)

De esta forma, estos prejuicios están dirigidos siempre hacia el mismo sector de la población: jóvenes, pobres, desocupados, inmigrantes, hijos de la desestructuración social de los años 90, con su derrotero de exclusión social y miseria.

Asimismo cabe destacar que la denominada "criminología mediática" colabora en conformar y se empeña en difundir estos estereotipos. En palabras de Zaffaroni, consiste en la "creación de una realidad a través de información, subinformación y desinformación en convergencia con prejuicios y creencias basadas en una etiología criminal simplista…".(4)

Podríamos arriesgar que la criminología mediática es un aspecto más de la mencionada selectividad, donde los medios de comunicación ocupan el lugar de usina ideológica imponiendo sus paradigmas, que muchas veces terminan por constituirse en política criminal ante la sumisión de los poderes políticos a los llamados "empresarios morales".

En base a estos conceptos estructurantes, entendemos que las personas detenidas no lo están tanto por el hecho cometido (o imputado), sino por sus características personales y/o por la coyuntura social que los atraviesa. En esta línea es que concebimos las limitaciones de nuestra intervención,

(3) Zaffaroni, Raúl; Alagia, Alejandro y Slokar, Alejandro, *Derecho Penal, parte general,* Bs. As., Ediar, 2005, p.10.

(4) Zaffaroni, E. Raúl, *La cuestión criminal,* Bs. As., Planeta; 2011; p. 210.

entendiendo que solo un cambio estructural haría posible concebir otra forma de sistema penal y otro proyecto de vida para los selectivizados.

Ahora bien, sin perjuicio de ello, cabe indagar en el margen de libertad de los sujetos **prisionalizados**. En este sentido, creemos que es necesario conjugar dialécticamente los factores macro-sociales y micro-sociales con la dimensión individual.

En lo que hace al nivel macro-social, debemos pensar fundamentalmente en el fenómeno de la selectividad penal, atravesada por las desigualdades económicas y sociales.

Luego, en la esfera de lo micro-social, es necesario explorar e indagar el devenir de la trayectoria vital de cada sujeto (relaciones familiares, antecedentes educativos y laborales, situación de salud, entre otras), ya que la intervención micro se da en el encuentro entre sujeto, sociedad y cultura, en cada circunstancia singular.(5)

En la dimensión individual, destacamos que si bien la población con la que trabajamos tiene características comunes, entendemos que cada sujeto atravesó sus propias encrucijadas y tomó diferentes decisiones. Debemos, entonces, pensar lo común sin anular lo singular, escuchando en cada sujeto eso que lo hace distinto de los demás, eso que lo hace **persona** antes que **preso**, **sujeto** antes que **objeto**.

Son muchos los interrogantes que emergen en el marco de nuestra labor. Así nos hemos preguntado: ¿todas las personas privadas de su libertad son iguales y sufren por lo mismo y de la misma manera?; ¿la pobreza, la marginalidad y la violencia influyen de igual modo en todos los casos?; ¿es posible trabajar en un juego dialéctico entre la selectividad que opera en la escala micro-social y la subjetividad particular de esta persona en concreto con la que nos encontramos?

Entendemos que es cierta particularidad respecto del deseo lo que nos hace **sujetos** capaces de elegir, responsabilizarnos e incidir en el propio destino. El orientarse hacia esa particularidad es lo que le devuelve su

(5) Carballeda, Alfredo, *La intervención en lo social. Exclusión e integración en los nuevos escenarios sociales*, Bs. As., Paidós, 2002.

dignidad al sujeto.[6] Estamos aquí en el terreno del "caso por caso", en el que para cada uno los determinantes individuales, familiares y sociales fueron distintos e incidieron de manera singular. En este proceso surgen diversos interrogantes: ¿qué significa para cada uno estar preso?, ¿con qué mandato inconsciente se está queriendo cumplir en este entrar y salir constantemente de la cárcel?, ¿qué busca alguien que necesita someterse una y otra vez a la ley caprichosa y cruel de **la tumba**?

Entonces bien, creemos que a partir de nuestra labor es posible, al menos, incidir en el plano individual, en los factores que condicionan su predisposición a ser selectivizados por el sistema penal. En este sentido, nuestros objetivos tienden a que el sujeto pueda posicionarse de otro modo, aún dentro de las limitaciones estructurales.

Esta práctica se inscribe en la denominada "atención interdisciplinaria de la vulnerabilidad psico-social" —también conocida como "clínica de la vulnerabilidad"—, que procura construir redes vinculares y grupales que protejan al sujeto del riesgo social, teniendo como objetivo el egreso, el menor tiempo de retención y las mejores condiciones para su reinserción familiar y socio-comunitaria.[7]

Es importante destacar que centramos nuestros mayores esfuerzos en desviar la atención de la acción delictiva o infractora, y colocarla en la reducción de la vulnerabilidad psico-social de las personas asistidas.

Nuestra intervención se orienta a reducir los efectos devastadores del encierro, en el marco del respeto por los Derechos Humanos y, sin pretender impulsar cambios sustantivos en la vida del sujeto, acompañarlo en la problematización de algunos de los aspectos que condicionan su vulnerabilidad psico-social. Se trata de iniciar la deconstrucción de su identidad estigmatizada, apuntando a la resignificación de algunos aspectos causantes de su sufrimiento. En esta lógica, al centrarnos en la especificidad de la persona, elegimos prescindir de la utilización de ciertos dispositivos

(6) Cabe aclarar que si bien desde el léxico de la psicología, se habla de "sujeto" en tanto la persona se encuentra escindida entre su parte conciente e inconsciente, se encuentra "sujeto" a este segundo aspecto que no domina desde su faz consciente.

(7) Domínguez Lostaló, Juan Carlos y Di Nella, Yago, *¿Es necesario encerrar?;* Bs. As., Koyatun, 2007.

de cálculo, evaluación y clasificación tendientes a cosificar, una vez más, al sujeto. Consideramos que, apoyándose en una supuesta homogeneización y un trato igualitario de las personas, estas prácticas indicadas como "evaluativas" (pero que encierran un contenido de control) tienden a reducir al sujeto a una cifra, ocultando el objetivo último del puro y simple ejercicio de poder. Por el contrario, desde nuestro trabajo se busca armar un vínculo opuesto al que se desarrolla con los profesionales de los consejos correccionales, donde se monta un "como si" solo orientado a la búsqueda de guarismos.

En esta línea, es importante destacar que si bien no desconocemos en absoluto los beneficios que aporta a la persona detenida avanzar en la progresión del Régimen Penitenciario, no centramos nuestra intervención en la "adaptación", entendida como la modificación del individuo respecto a las condiciones del medio en el que vive. En este sentido, entendemos que la cárcel es un entorno completamente hostil y en modo alguno apto para el desarrollo del sujeto, por lo que la adaptación a él acarrearía consecuencias negativas y muchas veces irreversibles.

Vale recordar una vez más la paradoja implícita en esta clase de sanciones: esperar la mejor inserción en el medio libre, desde el encierro. Sin perjuicio de ello, en el marco de los encuentros, procuramos problematizar las opciones que brinda el ámbito carcelario para que el sujeto pueda disponer del margen de libertad y opción que se le quita.

Como profesionales del campo psicosocial intervenimos desde nuestra especificidad, cuando escuchamos a alguien que sufre, alojando y dando un tratamiento a su angustia que, como dijimos, va a ser distinto en cada caso.

Es fundamental propiciar un cuestionamiento profundo en el sujeto que ayude a generar el pasaje de la simple queja por "lo que me pasó" a la pregunta de "qué hice yo para que me pase esto", o "por qué hice aquello si sabía que me pasaría esto". El profesional se ofrece como soporte para que esta pregunta surja, y acompaña al sujeto en la formulación de una o varias respuestas posibles. El valor que tiene esta pregunta es doble: por un lado, permite comenzar un trabajo de análisis y reconstrucción de las experiencias del sujeto y las consecuencias que de ellas derivaron, y por el otro, afianza el vínculo con los profesionales. Esto último se fundamenta en que la pregunta, en apariencia dirigida a otro, interroga en verdad a quién la formula.

Ello es el producto de varios encuentros en los que este vínculo se va construyendo y, a su vez, es el punto de partida para un trabajo más arduo, con constantes avances y retrocesos. Muchas veces es la misma persona quien se presenta simplemente como "un preso" o "un tumbero", identificándose fuertemente con esta imagen y tornándola inconmovible. Pero si partimos ahora de la suposición de que "ser un preso" es mejor que "ser nada", esta identificación parece cobrar cierta coherencia, a pesar de acarrear muchas consecuencias negativas. Este fenómeno fue abordado por la corriente criminológica de las "subculturas criminales" que describe cómo la pertenencia a estos grupos no implica necesariamente un esfuerzo por contradecir el sistema de valores vigentes, sino que tiene sus propios conjuntos de valores, sus jerarquías y sus reglas. Tal como lo describió Albert Cohen, entre otros, se trata de una delincuencia expresiva y no instrumental, que no pretende la mera satisfacción de necesidades materiales.

Una novedad que incorpora la teoría de las subculturas estriba en afirmar que estos colectivos sociales organizados y "desviados" no profesan la misma escala de valores que el resto de la sociedad. De hecho, la denominación subcultura refiere a entramados culturales diversos, que se diferencian *ex profeso* de los valores convencionales de clase media, en la intención de construir subjetividades y afirmar una identidad que el propio sistema les escamotea.

Ello debería ser muy tenido en cuenta por quienes nos desempeñamos en ámbitos carcelarios: muchas veces eso que hace sufrir a alguien es lo mismo que lo sostiene y lo único que le da una razón de ser, por lo que estamos obligados a respetar los tiempos y posibilidades subjetivas de las personas con las que trabajamos.

Como Equipo Interdisciplinario entendemos que el sufrimiento de quien está detenido no se reduce solo a su causa penal, sino que está condicionado por múltiples factores. Nos proponemos entonces acompañarlo a desentrañar esos motivos, aunque sea en parte, re-escribir la propia historia, desandar a través de la palabra ese camino que lo lleva una y otra vez al mismo lugar. Para ejemplificar: si uno no sabe por qué hace las cosas que hace o le pasan las cosas que le pasan, difícilmente pueda modificar en algo su situación; por lo tanto, seguirá una y otra vez actuando "a ciegas", repitiendo hasta el infinito sus actos y sufriendo eternamente las consecuencias.

Si bien la escucha en sí misma no posee carácter curativo, la escucha de alguien que supone en el otro un sujeto capaz de ser agente de sus actos y no un mero objeto o una víctima del sistema, puede humanizar a quien se encuentra inmerso en instituciones inhumanas. En este sentido, creemos que, una vez que este dispositivo se instala, estarían dadas las condiciones para que se produzca un nuevo tipo de lazo social, otra manera de "pensarse con los otros".

3 | La intervención del Equipo

3.1 | Nuestra actividad

Como bien se ha señalado, la característica primordial de nuestra intervención es el prisma del "de a uno" o "caso por caso", lo que resulta definitivamente opuesto a la manera en que se interviene habitualmente con las personas detenidas, atendiendo a esta población como una masa de gente deshumanizada e indiferenciada.

Nos centramos en brindar atención psicológica y social a las personas detenidas, manteniendo un vínculo con ellos a través de entrevistas individuales que se llevan a cabo con una frecuencia semanal. Así se atienden sus necesidades y demandas de índole psicológica y social, ya sean originadas por la misma situación de encierro o por motivos preexistentes. Asimismo, en forma periódica, se realizan encuentros con su familia y allegados.

Por otro lado, como parte del proceso de intervención social, se realizan articulaciones intra e inter institucionales —con organismos públicos, privados y del tercer sector— con la finalidad de gestionar los recursos sociales existentes dentro de los distintos ámbitos.

Se destaca que en forma concomitante llevamos a cabo una actividad de monitoreo permanente de la situación de encierro, a través de estas visitas semanales durante todo el lapso de permanencia en la unidad.[8] De esta manera se toma conocimiento concretamente y en tiempo oportuno de

(8) Debemos remarcar que la ausencia de una política penitenciaria en la Ciudad de Buenos Aires trae como consecuencia que las personas se encuentren alojadas en el sistema federal, distribuidas por distintos complejos y unidades del conurbano e incluso del interior del país.

cualquier tipo de inconveniente que se le presenta al asistido, ya sea sobre su situación de detención, relación con sus compañeros de pabellón, vínculo con los agentes del Servicio Penitenciario, como también las peticiones, demandas o planteos que formule. Esta información es transmitida en forma inmediata al defensor el mismo día que se produce la visita, con el objetivo de que pueda conocer las novedades y en base a éstas efectuar las eventuales presentaciones judiciales, o bien readecuar su estrategia de defensa si lo considera necesario. En estos aspectos, nuestra labor está en línea con los postulados de las "Reglas de Brasilia", en cuanto promueve el acceso a la justicia de una población específicamente vulnerable, como lo es la población detenida en establecimientos penitenciarios.(9)

Como parte de la Defensa Pública, el Equipo tiene presente en todo momento la importancia de resguardar y afianzar la relación entre el detenido y su defensor técnico. Una adecuada relación de confianza entre ambos incide positivamente en el estado emocional del detenido, al reducir el nivel de ansiedad y, concomitantemente, la posibilidad de sufrir irrupciones de angustia o de incurrir en *actings* que lo podrían exponer a diversas consecuencias negativas, como sanciones disciplinarias o problemas de convivencia con sus pares. Asimismo, esta relación de confianza facilita la apertura de un espacio de trabajo y reflexión sobre aspectos psicosociales.

Por otro lado, nuestra tarea contempla la producción de informes socioambientales, psicosociales y/o psicológicos que den cuenta de la situación de la persona detenida.

Es importante señalar que la propuesta de este Equipo apunta a ocupar un lugar hasta el momento vacante en materia de políticas activas, destinadas a asistir a las personas en conflicto con la ley penal, debido a la carencia de instituciones dedicadas prioritariamente al acompañamiento profesional de esta población.

En estas condiciones, con los detenidos en el sistema federal, la Ciudad tampoco genera políticas post-penitenciarias ni pone a disposición recursos específicos.

(9) Vale aclarar que ninguno de los profesionales del Equipo Interdisciplinario —aunque se trate de abogados— brinda asesoramiento jurídico. Ello está expresamente prohibido por la resolución que regula el funcionamiento del área. Cuya participación se limita al abordaje psico-social y tiene como objetivo aportar un plus a la Defensa y por tanto evita la superposición de roles.

3.2 | Metodología

El trabajo del Equipo se encuentra estructurado en un programa organizado a partir del desarrollo de tres etapas articuladas entre sí, que describimos sintéticamente a continuación. El **primer momento** de la intervención se encuentra orientado fundamentalmente a acompañar a la persona a transitar el inicio de su situación de detención y los efectos disruptivos que esta circunstancia habitualmente produce; por ejemplo, la aparición de sensaciones de incertidumbre, desborde y desamparo afectivo, desorientación temporal y espacial, entre otros.

En términos generales, se trata de un momento de honda crisis personal y subjetiva, frente a la cual se trabaja psicológicamente siguiendo los tiempos y exigencias impuestos por el escenario de la urgencia. Se busca así instaurar un espacio terapéutico que facilite la reflexión y la contención emocional.

Asimismo, se focaliza la atención en brindar acompañamiento y orientación emocional, posibilitando la tramitación de altos niveles de ansiedad y angustia que caracterizan el primer momento de detención, específicamente cuando la situación procesal o judicial no está definida o hay apelaciones pendientes que generan una situación de gran tensión. Desde la especificidad del trabajo social, y guiados por el objetivo de promover la restitución de derechos históricamente vulnerados, es que concebimos al sujeto en su aspecto relacional.

En este sentido, trabajamos en base al aparato de "protección social"[10] del Estado,[11] es decir, el conjunto de las políticas públicas existentes con las dificultades que aparejan las deficiencias presentes en el ámbito de la Ciudad. En base a los medios disponibles se realizan gestiones de recursos sociales, especialmente trámites de documentación que son necesa-

(10) En efecto, el aparato de "protección social" cumple con un doble sentido: desde el punto de vista de la sociedad en su conjunto, coadyuva a la reproducción de la fuerza de trabajo mientras que, desde el punto de vista de las personas, compromete directamente las necesidades materiales de reproducción. En ese cruce, se abre el terreno a la lucha social y política. Véase Hintze, Susana y Danani, Claudia (coords.), *Protecciones y desprotecciones, la seguridad social en Argentina*. 1990-2010; UNGS; Colección Política, Políticas y Sociedad, nº 08, 2011, p. 14.

(11) *Ibid.*

rios para que una persona pueda insertarse en las actividades que brinda el lugar de detención (trabajo, estudio, salud, visitas, etc.).

Desde el primer momento de la detención, se entrega mensualmente a la persona detenida una tarjeta telefónica. El objeto de ello es que pueda comunicarse con sus allegados y sostener los lazos afectivos que promueven su contención emocional, y con su defensor, para así evacuar sus dudas sobre su situación procesal, cuando lo requiera.

En la misma línea, durante todo el período de detención, la Defensoría General, a través del Equipo Interdisciplinario, solventa los viáticos para las visitas que efectúan los allegados a los lugares de alojamiento, con el mismo objeto de facilitar el sostenimiento de los lazos afectivos.

Una **segunda etapa** de intervención, está determinada por tres factores concomitantes: el consentimiento del sujeto, la consolidación de un vínculo o alianza terapéutica con los profesionales a cargo, y el sostenimiento del mismo.

Según el tipo de problemáticas específicas presentadas por la persona en situación de encierro, la intervención psicológica podrá asumir metodológicamente distintas modalidades, que bien podría ser una terapia de corte psicoanalítico u otros modelos de tratamiento, siempre con el máximo respeto de la confidencialidad y la voluntad del asistido.

Desde el trabajo social, se presta especial atención a que la persona pueda cumplimentar las exigencias de las distintas etapas de la ejecución penal con miras a obtener la libertad. Así, las entrevistas comienzan una vez que se cierra la puerta (en caso de que haya una, claro está)[12] y se realizan intentando mantener la mayor privacidad posible entre el profesional y el asistido, evitando la intromisión de los guardias.

De este modo se plasman materialmente los lineamientos de consentimiento informado y confidencialidad, que constituyen el eje del vínculo terapéutico.

(12) Se destaca al respecto la situación que se da en el Complejo Penitenciario de la Ciudad Autónoma de Buenos Aires (ex Unidad N° 2), donde a raíz de nuestras prácticas cotidianas y de la presencia permanente, en vez de realizar las entrevistas en la "leonera" de la Sala de Abogados, se nos permite utilizar la Sala de Ejecución Penal, que otorga un marco más adecuado a las condiciones de privacidad mencionadas.

El resultado de estos presupuestos es la reacción inesperada de las personas privadas de su libertad cuando son visitadas por un equipo que llega a la cárcel desde la Defensoría General de la Ciudad y les informa que la frecuencia de los encuentros será semanal, que lo que se diga allí queda bajo estricto secreto profesional (salvo que haya un pedido explícito de transmitir alguna información urgente a su Defensor/a), y que además se les aclara que dicho espacio es optativo.

El Equipo Interdisciplinario trabaja en el convencimiento de que la persona privada de libertad encuentra cercenado su derecho a gozar de libertad ambulatoria, más no de los restantes derechos que lo amparan. Más aún, cuando la persona se encuentra privada de su libertad, el mismo Estado deviene en garante de sus derechos, con lo que reposa en este la obligación de que su derecho a la salud (y específicamente a la salud mental) sean efectivizados.

El esfuerzo de nuestro Equipo se orienta a plasmar estos postulados en el trabajo diario, en el anhelo de que en el futuro pueda constituirse en el marco de acción de todos los profesionales intervinientes.

4 | Conclusiones

Luego de este recorrido por nuestra labor, cabe destacar una vez más, que trabajamos sobre la articulación entre, por un lado, el contexto social en el que se inserta un sistema penal selectivo y, por el otro, el margen de libertad de los sujetos, propio de la lógica de cada caso. Es así que partiendo de estas premisas, nuestra intervención se propone reducir los niveles de vulnerabilidad de las personas asistidas, incidiendo en los aspectos psicológicos y sociales, en el entendimiento de que dicha reducción tendrá como consecuencia directa que los destinatarios sean menos propensos a la criminalización ejercida por el sistema penal. Y, en definitiva, que sean menos vulnerables a la criminalización. Para finalizar, resulta por demás interesante citar un aporte del criminólogo Alessandro Baratta que condensa las aspiraciones de este Equipo:

> "Cualquier paso que pueda darse para hacer menos dolorosas las condiciones de vida en la cárcel, aunque sea solo para un condenado, debe ser mirado con respeto cuando esté realmen-

> te inspirado en el interés por los derechos y el destino de las personas detenidas, y provenga de una voluntad de cambio radical y humanista y no de un reformismo tecnocrático cuya finalidad y funciones sean las de legitimar a través de cualquier mejoramiento la institución carcelaria en su conjunto".[13]

Consideramos que este fragmento introductorio condensa gran parte de lo que inspira el trabajo del Equipo de Intervención Interdisciplinaria respecto de las personas privadas de su libertad que están a disposición del Poder Judicial de la Ciudad de Buenos Aires. Una vez por semana caminamos por las prisiones de Marcos Paz, Complejo Penitenciario de la Ciudad Autónoma de Buenos Aires (ex Unidad N° 2) y Ezeiza, entre otros dispositivos carcelarios, intentando dar ese paso que ayude a disminuir los efectos de la prisionalización en el conjunto de la población asistida.

(13) Baratta, Alessandro, *Resocialización o Control Social. Por un concepto crítico de la reintegración social del condenado*; Universidad de Saarland, República Federal de Alemania, 1993; Rivera Beiras, Iñaki, "Estrategias para una transformación radical y reduccionista de la cárcel. Un programa de reducción de daños desde y con la sociedad civil", Universidad de Barcelona, mimeo, 19 de abril de 2012.

Organización judicial

Es conocida la afirmación de Ernst von Beling de que "el derecho penal no toca un solo pelo al delincuente". Se podría agregar que el derecho procesal penal sí lo hace y que, en la mayoría de los casos, el procedimiento y las cuestiones de organización suponen para él un verdadero padecimiento.

Precisamente, dado que esta rama del derecho trata con los bienes más preciados de los ciudadanos, las decisiones deben estar rodeadas de ciertos requisitos y, para ello, se han dispuesto determinados recaudos. Se requiere que las decisiones detenten cierto nivel de valor de verdad y, a ese fin, resulta ineludible que toda resolución definitiva de un juicio cuente con una revisión posterior, como modo de lograr una mayor seguridad sobre la justicia del destino del acusado. En materia penal, la suerte de una persona no puede estar librada a la decisión de un solo funcionario u órgano estatal.

No obstante ello y, paradójicamente, bajo ciertas circunstancias el ejercicio mismo de ese "derecho a una revisión amplia de la sentencia" conlleva efectos nocivos o perjudiciales para la persona que se encuentra sometida a un proceso penal. En particular, la dilación en la resolución de los recursos constituye uno de los mayores déficits del actual modelo de organización judicial, dado que habitualmente los tiempos que insumen los trámites recursivos llegan a superar el de investigación o juzgamiento, cuando no el de la conjunción de ambas etapas del procedimiento.

En esta oportunidad, se presentan dos escritos relativos a formas de organización del trabajo en el ámbito recursivo, con el denominador común de que en ambos casos se abordan modelos de procedimientos de revisión cuya tramitación y resolución implica la realización de audiencias orales.

Uno de ellos referido a la implementación de la ley 26.374 por parte del Cámara Nacional de Apelaciones en lo Criminal y Correccional de la Capital Federal ("Cámara del Crimen") que, en nuestro país y bajo un sistema inquisitivo, constituye la saludable excepción del único tribunal que —so-

metido a la reforma— la aplicó, dado que la gran mayoría de las cámaras de apelaciones federales han dictado actos administrativos en virtud de los cuales simplemente desconocieron la reforma legislativa y se mantienen en un estado de alzamiento frente a la ley.

El otro aporte consiste en un estudio sobre el sistema recursivo imperante en la Ciudad de Santiago, Chile, país que cuenta con un modelo procesal adversarial y un modelo de organización y gestión judicial moderno. Este relevamiento da cuenta de una experiencia que, como se viene remarcando desde esta sección respecto de diversos aspectos, constituye un material valioso a fin de modernizar nuestro arcaico sistema recursivo.

Siempre deseando que estos aportes ayuden a la reflexión y den impulso a la tan necesaria modernización del sistema de enjuiciamiento penal, en pos de que se garanticen los derechos ciudadanos que la Constitución Nacional —desde su formulación originaria de 1853— pretende proteger.

Santiago Martínez, Diego García Yomha,
Nahuel Martín Perlinger y Juan Pablo Iriarte

Colaboradores Sección Organización Judicial

La reforma de la ley 26.374

Su aplicación en la Cámara Nacional de Apelaciones en lo Criminal y Correccional de la CABA[1]

por **TAMARA PEÑALVER**[2]

"Este procedimiento judicial, y este método de castigo, que usted tiene ahora oportunidad de admirar, no goza actualmente en nuestra colonia de ningún abierto partidario. Soy su único sostenedor, y al mismo tiempo el único sostenedor de la tradición del antiguo comandante. Ya ni podría pensar en la menor ampliación del procedimiento, y necesito emplear todas mis fuerzas para mantenerlo tal como es actualmente. En vida de nuestro antiguo comandante, la colonia estaba llena de partidarios; yo poseo en parte la fuerza de convicción del antiguo comandante, pero carezco totalmente de su poder; en consecuencia, los partidarios se ocultan; todavía hay muchos, pero ninguno lo confiesa".
Franz Kafka[3]

(1) Quiero agradecer a Ignacio Andrioli y a Gabriela Ortiz por su colaboración en el relevamiento de audiencias, ya que sin ellos esta publicación no hubiera sido posible.

(2) Estudiante de Derecho en la Universidad de Buenos Aires. Investigadora del Instituto de Estudios Comparados en Ciencias Penales y Sociales (INECIP).

(3) Kafka, Franz, "En la colonia penitenciaria", en *Relatos completos*, Madrid, 2004.

I | Introducción

Desde hace más de 20 años los procesos de reforma en América Latina se han afianzado y han logrado profundas modificaciones en los sistemas de administración de justicia. Podemos acudir a ejemplos de países vecinos que han abandonado sistemas inquisitivos para adoptar procesos completamente acusatorios como el caso chileno.[4] También podemos mencionar modelos nacionales, como la provincia del Chubut,[5] que ha conseguido establecer un verdadero sistema procesal penal moderno que cumple en gran medida con el diseño constitucional de nuestro país.

No obstante la Argentina tiene una gran deuda pendiente, y esa deuda se hace llamar "Justicia Federal". Este sistema permanece incólume desde la sanción del Código Levene en 1992, independientemente de algunas modificaciones que sufrió y que hoy lo convierten en una legislación poco uniforme remendada por leyes posteriores a su sanción. Sin embargo, dentro de estos parches legales, cabe destacar que en el año 2008 se produjo una importante reforma al Código Procesal Penal de la Nación (en adelante, CPPN). La ley 26.374[6] introdujo cambios radicales en el modo de tramitar los recursos de apelación[7] en la justicia federal y en la justicia nacional en lo criminal y correccional. Dicha ley estableció que las apelaciones ya no se resolverían por escrito sino mediante audiencias orales y públicas.

Por primera vez, nuestro sistema federal de corte mixto, cuya etapa de instrucción era plenamente escrita, encontraría en las apelaciones la excepción a la regla: la oralidad. Esta característica propia de los sistemas acusatorios, funcionaría como un verdadero mecanismo para la toma de decisiones judiciales en la etapa previa al juicio. En este sentido, Alberto Binder,[8] entien-

(4) AAVV, "Reformas Procesales Penales en América Latina", en *Revista Sistemas Judiciales,* nº 3, 19/08/2002, p. 18.

(5) Ley 5478, Código Procesal Penal de la Provincia del Chubut.

(6) Sancionada el 21 de mayo de 2008. Comenzó a regir el 29 de agosto de 2008.

(7) Además, la reforma modificó el modo de tramitar el recurso de casación mediante la implementación de audiencias orales y públicas para su resolución (entre otros cambios). Cabe destacar que el presente documento está destinado exclusivamente al análisis del recurso de apelación, es por ello que se hace especial hincapié en este.

(8) Binder, Alberto, "Introducción al Derecho Procesal Penal", Bs. As., Ad-Hoc, p. 72.

de que la oralidad es un instrumento que sirve para preservar los principios políticos y garantías que estructuran el sistema penal. En el mismo marco, afirma que la oralización y la incorporación del litigio en el trámite del recurso aparecen como prácticas con capacidad de abrir brechas en la tradición inquisitorial.(9) Es así que ateniéndonos al caso particular podemos concebir que esta reforma, aunque parcialmente, se produjo para intentar romper con la cultura inquisitiva que define las prácticas de nuestro sistema de justicia.

Es por ello, que el propósito de este trabajo es mostrar cómo se desarrolla la innovación en cuestión cinco años después de su sanción, para reflexionar sobre el real tratamiento y gestión de las audiencias que llevan a cabo los tribunales involucrados en la reforma y para poder localizar los principales avances y deficiencias en la implementación de esta ley.

Para llevar a cabo esta tarea, se ha realizado un relevamiento de audiencias en la Cámara Nacional de Apelaciones en lo Criminal y Correccional de la Ciudad Autónoma de Buenos Aires.(10) Se ha elegido este tribunal debido a que es el que por excelencia ha cumplido con este desafío, que dentro de las actuales prácticas coloniales que rodean la actividad recursiva, debe considerarse como una verdadera manifestación de voluntad política destinada a mejorar la calidad del servicio de justicia.

Se han observado un total de treinta audiencias, seis por cada sala de dicho tribunal, con el fin de analizar las actuaciones judiciales y circunstancias que hacen al desarrollo y cumplimiento de la normativa. También en el marco de la investigación, se ha entrevistado a personal de la Cámara con el fin de ahondar en la lógica de la organización y distribución de trabajo.

En un primer apartado, se hará una breve mención al modo en que se encontraba regulado el tratamiento de los recursos de apelación previamente a la reforma y a cómo se regula en la actualidad. Posteriormente, se volcará la información relativa al relevamiento de audiencias, incorporan-

(9) Binder Alberto, "La fuerza de la inquisición y la debilidad de la república", en *La implementación de la nueva justicia penal adversarial*, Bs. As., Ad-Hoc, 2012, p. 33.

(10) En relación a las demás cámaras, algunas han escogido transformar la obligación de realizar las audiencias en una mera opción para el recurrente. Otras eligieron diferir la efectiva aplicación de la ley a través de acordadas que afirman la imposibilidad de su cumplimiento (CNac. Apel. Crim. y Correcc. acordada 59/2008).

do datos cuantitativos y cualitativos respecto de su gestión en la Cámara del Crimen. Ello sin el fin de realizar duras detracciones a este tribunal, sino por el contrario, con el fin de instaurar un sentido crítico, brindando información sobre el real funcionamiento de la inmediación, la publicidad, la celeridad y la contradicción que deberían generarse a partir de la implementación de las audiencias orales.

Este trabajo finalizará con el desarrollo de una serie de conclusiones sobre el material expuesto y propondrá posibles acciones de cambio a aquellas prácticas que lejos estén de lograr un sistema de enjuiciamiento penal de calidad.

2 | Los recursos de apelación: antes y después de la reforma

Nuestro Código Procesal Penal de la Nación al tratar los recursos de apelación establece que procederán contra los autos de sobreseimiento dictados por los jueces de instrucción y en lo correccional, los interlocutorios y las resoluciones expresamente declaradas apelables o que causen gravamen irreparable.[11]

Antes de la reforma, estos recursos eran interpuestos por escrito ante el juez que había dictado la resolución impugnada, y debían contener —para ser admisibles— los motivos que lo fundamentaban. Una vez concedido el recurso y sorteada la Sala, las partes debían presentarse ante el tribunal de alzada, en el plazo de tres días, y mantener el recurso. Caso contrario, se tenía como desierto. Siempre que este tribunal diera lugar a la impugnación, se pactaba una audiencia en el plazo de cinco días desde las últimas actuaciones.[12] En dicha audiencia, las partes ampliaban los agravios, y podían optar por hacerlo en forma oral o escrita. La elección de la modalidad debía ser expresada al momento de ser notificados de la audiencia. Es decir, las audiencias orales no eran obligatorias y las partes tenían un plazo para elegir si querían realizarlas de ese modo.

(11) Art. 449 CPPN (vigente).

(12) Art. 454 CPPN (sustituido por ley 26.374).

En cuanto a la resolución de los recursos, correspondía notificar a las partes luego de cinco días de finalizada la audiencia,[13] plazo que pocas veces se cumplía, salvo en los casos en que la persona imputada se encontraba detenida.[14]

Este tipo de sistema recursivo verticalista, provocaba largas demoras en la resolución de las impugnaciones, por lo que los plazos se veían gravemente prolongados. En la generalidad de los casos previos a la reforma, los recursos eran tramitados en forma escrita y tardaban en resolverse entre ocho meses y un año.[15]

La sanción de la ley 26.374 tuvo como objetivo principal modificar en forma sustancial la tramitación de los recursos para evitar, entre otras cosas, los artilugios procesales que dilataban el proceso penal. En esta línea, la regulación de audiencias orales y públicas como nueva metodología para la resolución de impugnaciones, fue vista como la forma más eficiente para lograr este resultado.

En el debate parlamentario, que culminó con la sanción de la ley, se hizo fundamental hincapié en afirmar que los tiempos procesales se veían menoscabados por la lógica del sistema que impedía que las causas sean elevadas a juicio en forma rápida debido a la demora en la resolución de las apelaciones y la constante interposición del recurso durante la etapa de instrucción. Algunos de los legisladores mencionaron la necesidad de lograr mayor celeridad en el proceso para impartir justicia e insistieron en que los plazos de la etapa de instrucción jamás se respetaban. Por otro lado, se aseveró en aquel entonces, que la modificación al Código era indispensable para cumplir con el art. 8 de la Convención Americana de Derechos Humanos, y por ende, con el plazo razonable que allí se establece. Es así, que se sostuvo que el recurso de apelación era el más utilizado en

(13) Art. 455 CPPN (sustituido por ley 26.374).

(14) Gallagher Lucía, "Dinámica de las audiencias en la etapa recursiva prevista por la ley 26.374 modificatoria del Código Procesal Penal de la Nación. Gestión y asistencia en la organización de la Oficina Judicial. Fallas y aciertos de la ley 26.374. Problemas y propuestas", inédito, p. 4.

(15) Información que surge de las preguntas formuladas al personal que trabaja en la Cámara del Crimen.

el proceso penal y, en consecuencia, su resolución mediante audiencias, permitiría el respeto de la normativa internacional.[16]

Con todo ello, la voluntad del legislador estaba dirigida directamente a acortar los plazos y a generar un sistema de justicia que controle y haga respetar el tiempo procesal, ya que una de las características del proceso penal nacional es la falsa perentoriedad de los plazos y la dilación indebida del proceso evidenciando el poder del trámite por sobre el debate oral.

Si bien han sido modificados en gran proporción los artículos del CPPN que regulan el recurso de apelación, algunas circunstancias perduran. Podemos mencionar, por ejemplo, que los recursos deben interponerse primero por escrito ante el tribunal que dictó la resolución impugnada y la presentación debe contener los motivos en los que se funda el recurso bajo sanción de inadmisibilidad. Sin embargo, se ha eliminado el emplazamiento y la necesidad de que las partes mantengan el recurso ante el tribunal de alzada, lo cual favorece radicalmente al trámite recursivo.

Empero, a pesar de que el artículo que regulaba el emplazamiento fue derogado,[17] las actuaciones del fiscal de cámara respecto del recurso se encuentran vigentes y establecen que en el término de tres días éste debe manifestar si se mantiene o no la impugnación interpuesta por el agente fiscal o si adhiere en favor del interpuesto por el imputado. En conclusión, el único que debe exteriorizar la voluntad de mantener la apelación es el fiscal de cámara.[18]

También se ha modificado la facultad de poder interponer la apelación por vía de diligencia, es decir, la posibilidad de impugnar oralmente en secretaría al momento de ser notificado de una decisión, dejándose constancia de ello.[19] Tal modificación, deja como única posibilidad la interposición del recurso de apelación por vía escrita.

(16) Ver versión taquigráfica [en línea] http://www1.hcdn.gov.ar/sesionesxml/reunion.asp?p=126&r=8#126-8-9

(17) Art. 451 CPPN (derogado).

(18) Art. 453 CPPN (vigente).

(19) Amelotti Nicolás y Bahamondes Santiago, "La audiencias orales ante la Cámara del Crimen de la Capital Federal. Un análisis práctico de la reforma introducida por la ley 26.374", *en Revista jurídica La Ley,* 2009-F-1202, p. 2.

En este marco de transformaciones, sin dudas la imposición de resolver los recursos mediante audiencias orales y públicas es el cambio sustancial que introduce la reforma. La ley establece que siempre que el recurso no sea rechazado por el tribunal de alzada se debe decretar una audiencia, la cual no debe realizarse antes de los cinco días ni luego de los treinta días de recibidas las actuaciones. La audiencia se celebra con las partes que comparezcan, pero en caso de que el recurrente no asista a la misma, el recurso queda desierto. A simple vista, la normativa establece que para llevar adelante la audiencia sobre el recurso de apelación sólo se requiere la presencia del recurrente, pudiendo la contraparte no asistir sin afectar a la realización.

La norma también determina cómo debe desarrollarse la audiencia e instituye que se le otorga la palabra a los recurrentes (sin aclarar el orden de exposición en el caso de que existan dos recurrentes) para que motiven el recurso interpuesto, y además manifiesten las peticiones en cuestión. Sin embargo, se establece una clara delimitación a las actuaciones de la parte, estableciendo que no puede introducir motivos distintos o peticiones diferentes a las presentadas en el escrito de interposición del recurso. Más allá de la posibilidad que brinda de ampliar los fundamentos, no permite a la parte salir del objeto del escrito, salvo para desistir de algunos motivos al momento de la exposición.

Otorgada la palabra al recurrente, tiene la posibilidad de expresarse la parte que resiste el recurso, y luego ambas partes pueden ofrecer aclaraciones sobre lo discutido en la audiencia. También la ley establece que el juez que preside la audiencia tiene la facultad de interrogar a las partes, sin aclarar en qué circunstancia debe hacerlo, dejando la acción de preguntar a la discrecionalidad del juez.

Solo explica que los demás jueces que compongan el tribunal eventualmente pueden preguntar. En este ámbito, es importante señalar que el rol del juez en las etapas previas al juicio debe ser diferente al rol que debe cumplir en el debate oral. Es decir, el juez de audiencias preliminares debe ser activo para la resolución de determinados puntos en conflicto mediante el ejercicio de preguntas aclaratorias y de control del respaldo de la información. Además, debe asumir un rol dinámico en la conducción del debate para evitar la desviación de la discusión, y así lograr luego, una toma de decisión de calidad. Por el contrario, el juez de juicio oral, debe ser más

distante para que sean las partes quienes produzcan la información que allí se discute.[20] Aclarado lo anterior, y volviendo sobre los ejes de la reforma, cabe destacar que los jueces deben resolver el recurso en la misma audiencia luego del debate y con la sola presencia del secretario al momento de deliberar. Esto permite garantizar la inmediación y (en cierta medida) la no delegación de funciones. Aquí los jueces deben estar presentes para resolver, ya que la propia audiencia es la que genera la información de calidad. La única excepción a la resolución inmediata luego de finalizada la audiencia es que se trate de un caso complejo; en tal situación, los jueces podrán dictar un intervalo de cinco días para deliberar y resolver.

Ergo, la normativa señala que los jueces deben brindar los fundamentos por escrito dentro del plazo de cinco días de dictada la resolución cuando haya sido revocada la decisión o bien tuvieran nuevos motivos para mantener la medida impugnada, como así también, cuando la decisión no hubiera sido dictada por unanimidad.

Por último, la ley 26.374 dispone la creación de una oficina judicial que coadyuve a las cámaras en la organización de estas audiencias, lo que además permitiría generar unidad de criterio en las actuaciones y completa separación entre las funciones jurisdiccionales y administrativas.

3 | Reglamentación en la Cámara Nacional de Apelaciones en lo Criminal y Correccional de la CABA

La Cámara tiene su sede en la Ciudad Autónoma de Buenos Aires e interviene en los recursos interpuestos contra las resoluciones emanadas de los jueces nacionales en lo Correccional, en lo Criminal de Instrucción, de Menores y de Ejecución (en los casos de suspensión del proceso a prueba).[21]

(20) Asociación Internacional de Juristas Inter Iuris (en el marco del Programa de Apoyo al Fortalecimiento Institucional del Sistema Penitenciario de la República de Bolivia), "Manual de Litigación en Audiencias de Medidas Cautelares", p. 37. Elaborado por Leticia Lorenzo, Juan José Lima Magne, Enrique Maclean Soruco e Iván Lima Magne.

(21) Art. 24 CPPN (vigente). El artículo además agrega que la Cámara atenderá los recursos de queja por petición retardada o denegada por los mismos jueces y en las cuestiones de competencia que se planteen entre ellos.

En relación a su conformación, el tribunal está constituido por cinco salas que se integran del siguiente modo:[22]

TABLA 1. CONFORMACIÓN DE LAS SALAS DEL TRIBUNAL

Salas[22]	Jueces	Secretarios	Prosecretarios	Administrativos
Sala I	3	3	2	11
Sala IV	3	4	1	12
Sala V	3	5	1	16
Sala VI	3	4	-	15
Sala VII	3	3	-	18
Juez Presidente	1	-	-	-
Totales en la Cámara	16	19	4	72

Como se referenció en un comienzo, la Cámara Nacional de Apelaciones en lo Criminal y Correccional de la Ciudad Autónoma de Buenos Aires es la única de las cámaras que cumple con la reforma de la ley 26.374. Por el contrario, las demás cámaras han intentado (y logrado) paliar el efectivo cumplimiento de la reforma a través de acordadas que, entre otras cosas, afirman la imposibilidad de llevar a cabo audiencias por falta de recursos humanos, técnicos y edilicios[23] y porque la realidad de las vacancias en los cargos haría del sistema oral un proceso más lento.[24] Es decir, amparándose en diversos motivos que podrían afrontarse con la reorganización y gestión de los recursos, las restantes cámaras se rigen por normas ya derogadas.

(22) Datos extraídos de la página del Poder Judicial de la Nación que fueron ampliados en base a entrevistas con el personal de la Cámara, ya que en la página oficial los datos en cuestión no están actualizados. Cada Sala cuenta con otros funcionarios no discriminados en secretarios y prosecretarios, y personal de servicio. Además cuenta con personal llamado ujier que en principio se encarga de notificar a las partes y/o interesados la fecha de realización de las audiencias. No obstante, hoy en día algunas salas optan porque las diligencias sean llevadas a cabo por la oficina de notificaciones de la Corte Suprema de Justicia de la Nación. Por lo que algunos de los ujieres, en realidad, tienen la tarea de realizar las cédulas, y no de diligenciarlas.

(23) Gaitán, Mariano, "La oralidad de los recursos en el Código Procesal Penal de la Nación. Breve diagnóstico sobre su implementación y propuestas para avanzar en la reforma", p. 2.

(24) Martínez, Santiago, "La reforma de la ley 26.374, alcances y consecuencias", [en línea] http://www.pensamientopenal.com.ar/node/28064

Como antítesis, el Reglamento para la Jurisdicción en lo Criminal y Correccional de la Capital Federal[25] (en adelante, RJCC) regula las actuaciones que deben ser llevadas a cabo para la realización de las audiencias orales. Es así que determina que una vez recibido el proceso se comunica a las partes la Sala interviniente (la cual podrá pedir al juzgado de origen el expediente y la documentación necesaria para su examen) y se fija la hora y la fecha de la audiencia.

Las audiencias se inician conforme al orden de llegada y registro en mesa de entradas de la parte recurrente o adherente en función de las restantes audiencias fijadas por el tribunal para esa misma hora y fecha. Se hace excepción al inicio por orden de llegada cuando en alguna de las causas haya una persona detenida, cuyo recurso debe ser tratado con prioridad al resto.

Respecto de la composición de la Sala, en los casos en que el tribunal se encuentre conformado por dos jueces sea por recusaciones, licencias, vacancias u otra razón se hace saber a las partes esta circunstancia y se les pregunta si desean formular objeciones, ya que si fuera necesario (en caso de no llegar a un acuerdo entre los dos jueces) el restante integrante o el Presidente de la Cámara deliberará con sus colegas a partir de la escucha del audio de la audiencia para arribar a una decisión.[26]

Se determina que los jueces presentes en la Sala deben indicar quién será el tercer juez que intervendrá con su voto en caso de que sea necesario. Dentro de esta línea, el reglamento establece que si así lo precisaran los jueces, se dictará un receso para que interceda el tercer juez, escuche las grabaciones y si no tiene preguntas que realizar a las partes, delibere. En caso de que considere preciso realizar preguntas, se debe convocar de nuevo a las partes.[27]

(25) Ver reglamento [en línea] www.pjn.gov.ar

(26) Art. 36, inc. h. 4 RJCC. Por otro lado, el art. 36, inc. b. RJCC establece: "Si los votos emitidos en alguna causa, que tramite ante una Sala en donde haya jueces con licencias (sin que se encontrara reemplazo), no formaran mayoría, la Sala se integrará con el Presidente del Tribunal y, en su caso, por el Vicepresidente 1°, luego por el Vicepresidente 2° y, de ser necesario, por los restantes jueces de cámara por orden de antigüedad".

(27) Art. 36, inc. h. 4 y 5 RJCC.

Por otro lado, el reglamento regula que el apelante cuenta con 10 minutos para exponer los fundamentos del recurso, y los replicantes cuentan con 5 minutos, salvo circunstancias excepcionales en las cuales el Presidente de la Sala puede otorgarles una prórroga cuando exista cierta complejidad en el caso concreto. Las dúplicas y las respuestas deben ser breves en relación al tiempo previamente concedido a las partes.

Para finalizar, el reglamento instituye que la parte que solicite la entrega del audio deberá aportar el soporte digital a diferencia de la normativa que afirma que las copias deberán ser entregadas a las partes, sin mencionar el explícito requerimiento de entrega.[28]

4 | De las leyes a las prácticas, la hermenéutica y la debilidad de la ley

Este apartado se abocará a brindar una descripción general del trabajo administrativo y jurisdiccional observado en la Cámara Nacional de Apelaciones en lo Criminal y Correccional de la Ciudad de Buenos Aires.

Se hará especial hincapié en la labor cotidiana del tribunal y en la precisión de las condiciones existentes para la atención de las personas involucradas en el proceso penal. Esto incluye una descripción de las características edilicias y del desarrollo y gestión de las audiencias.

4.1 | Organización y actividades previas a la realización de las audiencias

Ante la falta de implementación de la Oficina Judicial, los preparativos que hacen a la realización de las audiencias dependen de cada Sala en particular. Si bien existe una oficina a la cual denominan "oficina judicial", esta no se responsabiliza por la carga de trabajo administrativo, ni centraliza las causas para la organización de las audiencias en cada una de las Salas. En síntesis, esta oficina no permite en la actualidad una verdadera separación entre las funciones jurisdiccionales y administrativas dentro del

(28) Ley 26.374, art. 11.

tribunal, y tampoco favorece a la unidad de criterio en las actuaciones. Por el contrario, la Sala de Turnos y Sorteos de la Cámara es la que recibe los casos y se encarga del trabajo administrativo de digitalizar los datos. Una vez que se realiza esta tarea, el mismo sistema es el que lleva a cabo el sorteo de la Sala que intervendrá en la causa.

Las propias Salas reciben los expedientes en su mesa de entradas y las personas que trabajan allí se encargan de analizar si corresponde o no admitir el recurso a partir del estudio de la presentación y del cumplimiento de las formalidades que requiere. Cuando finalmente el recurso es admitido, se fija la audiencia cuya fecha se determina teniendo en cuenta la complejidad de la causa y si en la misma hay personas privadas de su libertad.[29]

Los responsables de la Sala estudian los casos y realizan un primer análisis de los recursos estableciendo parámetros de tiempo y dificultad para calcular cuántas audiencias se pueden llevar a cabo en un día. Es por ello, que al momento de determinar día y hora, se pondera la cantidad de audiencias que podrán ser realizadas en una franja horaria determinada (por ejemplo, de 8.30 a 10.30 y de 10.30 a 12.30). Las partes deben presentarse en mesa de entradas o en una oficina de registro[30] y las audiencias se realizan según el orden de llegada de las partes citadas en esa franja horaria bajo la guarda de que aquellos casos con personas detenidas deben ser tratados con antelación al resto.

Habitualmente, los responsables de asignar los horarios de las audiencias[31] ordenan en primer lugar las causas con personas privadas de su libertad y luego toman en cuenta que sean los mismos defensores o fiscales los que deban estar presentes en varias audiencias, para asignar una tras

(29) Souto, Diego y Peluffo, Vanesa, "Fin de la Falsa Oralidad en la Cámara Criminal y Correccional de la Capital Federal. Nuevos desafíos hacia un sistema penal acusatorio", en *Revista de Derecho Penal y Procesal Penal*, Abeledo-Perrot, 2013.

(30) La única Sala que cuenta con una oficina de registro separada de la mesa de entradas es la Sala VII, ya que su mesa de entradas está en el primer piso y la sala de audiencias se encuentra en el quinto piso junto a la oficina de registro. Esta nueva oficina permite una mejor atención y organización con las partes.

(31) En general son secretarios y prosecretarios quienes realizan esta actividad.

otra con el fin de que litiguen en ellas en forma continua.[32] En conclusión, por ejemplo, si un defensor tiene que estar presente en tres audiencias, se intentan organizar una seguida de la otra para que la parte no salga de la sala hasta que finalicen todas sus actuaciones.

Quien se hace cargo de coordinar el audio, de acompañar a las partes y de supervisar el desarrollo de las audiencias es uno de los secretarios o prosecretarios de la Sala que es designado por día para organizarlas. También son los responsables de acomodar la sala de audiencias al final del día. Algunas de estas actividades las realizan en colaboración de empleados judiciales de la Sala. Sin embargo, siempre son entre una y dos personas las que se encargan de la totalidad de las audiencias del día.

En relación a las características edilicias, la Cámara carece en sus diversos pisos de espacios destinados específicamente a que las partes aguarden, por lo que los asistentes esperan a ser llamados a las audiencias en el pasillo correspondiente a cada piso.[33] En particular, se observó que varias personas no tienen un lugar para tomar asiento hasta ser llamadas y que no hay un espacio destinado a que aguarde la víctima y el imputado en caso de estar presentes.[34]

Dentro de las actividades jurisdiccionales previas a la realización de las audiencias, cabe mencionar que los secretarios encargados de coadyuvar en el caso particular reciben los recursos y arman un resumen de los hechos del caso que es entregado a los jueces al momento de la audiencia (o antes) para que lo lean y tengan una idea general de lo sucedido. Este resumen es denominado dentro del tribunal como "minuta" y está presente en todas las audiencias sea cual fuera la Sala a cargo. Aunque no solo está presente la minuta, sino que además está presente el expediente.

(32) Por ejemplo, una de las pocas audiencias en la cual se encontraba presente un familiar del imputado detenido, había sido pactada 8.30 hs. Sin embargo, como la abogada defensora tenía otra audiencia más tarde, la pactada para 8.30 hs. fue postergada hasta las 10.00 hs. aguardando el familiar en el pasillo hasta ser llamado.

(33) La excepción es la Sala VII que cuenta con un salón que es utilizado por todos los operadores de justicia y ciudadanos que asistan a las audiencias.

(34)Tampoco los pisos cuentan con baños públicos por lo que los empleados de la Cámara deben permitir a los asistentes usar los sanitarios privados de las Salas respectivas.

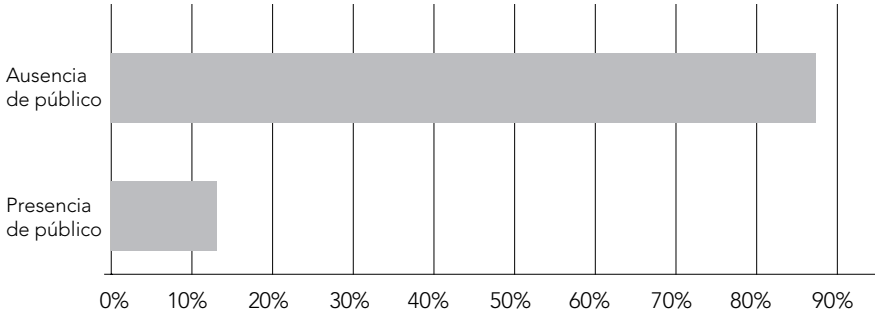
4.2 | La realización de las audiencias

4.2.1. Las salas de audiencias y la publicidad

Las cinco salas que conforman la Cámara tienen características similares. Todas son relativamente pequeñas con poco espacio para que pueda asistir público a las audiencias. En ninguna de las salas entran más de ocho espectadores. Algunas poseen, para los ciudadanos ajenos al proceso, solo tres sillas completamente pegadas a las de las partes que en caso de ser más de dos personas, deben usar los asientos del público reduciendo aún más los espacios libres.

En general, no asisten personas ajenas al litigio. Las excepciones (en pocos casos) son los familiares del imputado detenido que se presentan a las audiencias para favorecer a la posible recuperación de la libertad. Como resultado del total de audiencias relevadas, se observa que sólo en el 13% hubo personas ajenas a las partes. Esto es, solo tres audiencias fueron presenciadas por familiares de las personas imputadas y una por un abogado que asistió para ver cómo se desarrollaban las audiencias. El 87% de las audiencias carecía de público ajeno a las partes.

GRÁFICO 1. PÚBLICO DE LAS AUDIENCIAS



Público en las audiencias: Ausencia de público: 87% (26 audiencias). Presencia de público: 13% (4 audiencias).

En ningún lugar del edificio de la Cámara se puede observar un cartel que de publicidad a las audiencias que están por realizarse. Incluso no todas las Salas señalizan dónde se llevan a cabo las audiencias. Por lo que, no se establecen las condiciones necesarias para que la garantía de publicidad se cumpla de manera satisfactoria. Así se afecta a la legitimidad y al control público de los actos de gobierno que certifican la confianza y la transparencia en el sistema de justicia.

En cuanto al equipamiento de las salas de audiencias, estas cuentan con una computadora, y equipo de audio para grabar las voces. Como no se registran mediante videos, solo cuentan con micrófonos para las partes, y solo algunas salas para los jueces también. A su vez, la más pequeña de todas las salas de audiencias no requiere para el registro de voces contar con micrófonos debido a que el reducido espacio permite grabar sin dificultad. No poseen importante tecnología.

4.2.2. La puntualidad

Del total de audiencias relevadas, se pudo observar que el 70%[35] de ellas comenzó dentro del rango horario en que fueron pactadas y en forma puntual. Aquellas audiencias que empezaron tarde, nunca tuvieron más de una hora y media de atraso. Las causales de demora se debieron a problemas en la organización de las audiencias, ya que al pactarse varias dentro de un mismo rango horario se provocaba que si una de ellas iniciaba tarde, la demora se trasladaba al resto.

En casos menores, el motivo del retraso se debió a la llegada tarde del abogado recurrente. Para ellos se contempla media hora de atraso. Pasados los treinta minutos sin que la parte se presente, el recurso queda desierto. Esto pudo observarse en una audiencia en la cual había más de un defensor y uno de los que debía asistir al debate no llegó.

4.2.3. Las partes presentes

La reforma establece que para que puedan llevarse a cabo las audiencias debe estar presente obligatoriamente el recurrente, sin necesidad de que la contraparte asista. Esta regulación estimula que la contraparte que resiste el recurso no se presente y genere serios problemas en torno a las reales condiciones de contradicción, inmediación y producción de información. En relación a la presencia de las partes, es notorio que la mayor cantidad de recursos son interpuestos por los abogados defensores. Por consiguiente, la defensa tiene un rol preponderante en el trámite del recurso. Se pudo observar que, en el 67% de los casos, la defensa se encontraba sola en la Sala de audiencias sin su contraparte.[36] Es en estos

(35) 21 audiencias comenzaron puntuales en relación a la franja horaria y solo 9 comenzaron de manera impuntual.

(36) Esto a pesar de la Resolución PGN Nº 65/08, que autoriza a los fiscales generales a designar a sus secretarios como fiscales subrogantes *ad hoc*, para que se efectivice la presencia del MPF en las audiencias ante la Cámara.

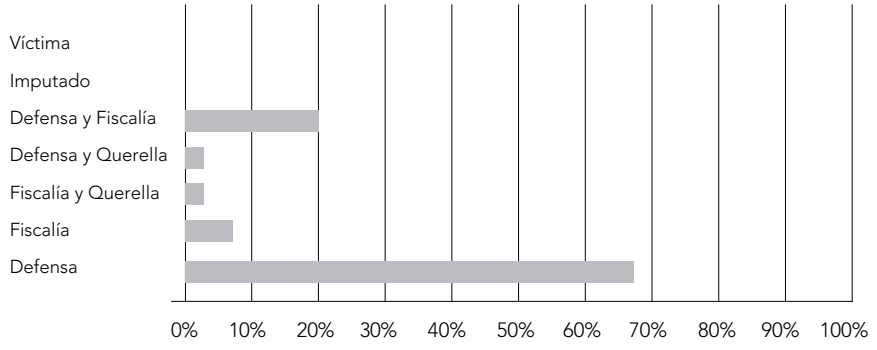
casos donde se tergiversa la posición del tribunal que concluye realizando preguntas al recurrente (en demasía) por creerlas pertinentes para poder tomar una decisión.

En suma, la ausencia de la contraparte no solo pone en crisis la contradicción que requiere cualquier audiencia para producir y controlar la información, sino que además genera un quiebre en los roles institucionales, ya que el tribunal pierde su calidad imparcial como conductor del debate con la potestad de decidir, para transformarse en una especie de parte.

En el siguiente cuadro se puede ver que en solo el 20% de las audiencias se encontraban presentes fiscales y defensores, y en el 6% se ubica la presencia de la querella con el defensor y el querellante con el fiscal. Estas audiencias sin dudas fueron las más ricas en contenido y producción de información y, fundamentalmente, en las cuales se apreció una verdadera división de funciones con una parte que requiere, una que resiste y otra que decide.

Independientemente de que estas audiencias previas al juicio se enmarquen en un sistema escrito que dificulta la implementación de una reforma íntegra y que genera la presencia del expediente en la resolución de los recursos, cabe destacar que la calidad de la información producida por las dos partes no puede compararse a la aportada en las audiencias en las cuales solo una de ellas estaba presente.

GRÁFICO 2. PARTES PRESENTES EN LAS AUDIENCIAS

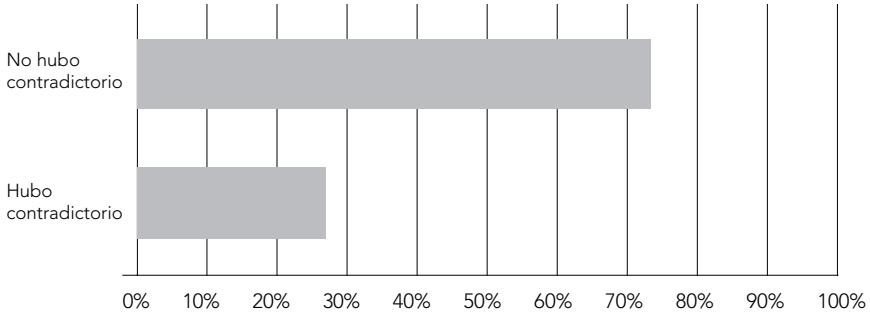


Partes presentes en las audiencias: Víctima: 0%. Imputado: 0%. Defensa y fiscalía: 3% (6 audiencias). Defensa y querella: 3% (1 audiencia). Fiscalía y querella: 3% (1 audiencia). Fiscalía: 7% (2 audiencias). Defensa: 67% (20 audiencias).

En aquellas audiencias en las cuales solo asistió el recurrente se observó que los jueces realizaban más preguntas y pedían aclaraciones sobre los hechos en cuestión. En general, los magistrados requerían a la parte información que no se brindaba en forma clara o bien le indicaban alguna foja del expediente que aludía al punto en conflicto. Tales acciones disminuían en grandes proporciones cuando ambas partes estaban presentes y debatían. En el 50% de los casos observados, los jueces no realizaron preguntas. En el restante 50% de las audiencias, los jueces efectuaron preguntas durante el desarrollo y finalizada la audiencia.

En lo relativo al contradictorio, se debe mencionar que en aquellas audiencias en las cuales las dos partes presentes mantenían intereses propios siempre existió debate y contradicción. En la única audiencia en la cual se encontraban presentes la querella y el fiscal, ambos mantenían peticiones diferentes por lo cual también fue contemplada en los porcentajes. Por cuestiones lógicas, en aquellas audiencias donde solo estaba presente la parte recurrente esto no sucedió.

GRÁFICO 3. CONTRADICTORIO EN LAS AUDIENCIAS



Contradictorio entre las partes: No hubo contradictorio: 27% (8 audiencias). Hubo contradictorio: 73% (22 audiencias).

4.2.4. La intervención de las partes

Las audiencias comenzaban con las palabras del secretario a cargo de la organización de las mismas, salvo excepciones, en las cuales el propio juez presidente de la Sala señalaba el número de causa, partes presentes y composición del tribunal.

Luego, se le daba la palabra al recurrente, que en no más de diez minutos debía desarrollar su fundamentación. A pesar de que así está regulado, los

alegatos de las partes pocas veces superaron ese límite y en esos casos los jueces no restringieron la palabra del apelante. En relación al contenido del alegato, como señalé previamente, la ley determina que no podrán ampliarse los motivos del agravio ni introducirse nuevos a los presentados en el escrito de interposición del recurso. Solo en una audiencia los jueces se opusieron a que el apelante continúe con su exposición por estar excediendo las demarcaciones del escrito. Por lo que, el apelante tuvo que volver sobre el eje de su presentación.[37] En el resto de las audiencias, los alegatos tenían plena relación con los motivos del agravio expuestos en el escrito de interposición del recurso.

El orden de exposición de los alegatos cuando existen dos partes que recurren, no está regulado por ley, por lo que la decisión al respecto corresponde a cada sala en particular. En el caso que se pudo relevar con la presencia de la querella y del fiscal, se comenzó por la exposición de la querella.

En el 97% de las audiencias los recurrentes alegaron oralmente los fundamentos y los motivos del agravio. La excepción fue una única audiencia en la que la parte recurrente se remitió al escrito de la impugnación y los jueces no se opusieron ni formularon preguntas. Como antecedente y en antagonismo con la actitud del tribunal en esta oportunidad, la Cámara en la causa "Rafael "[38] tuvo por desistido el recurso del apelante porque este se remitía al escrito de presentación del recurso sin ampliar oralmente los fundamentos. En aquella ocasión tras manifestar el tribunal que lo que no es introducido en la audiencia no puede entrar en el ámbito de la valoración y decisión, declaró desierta la impugnación.

4.2.5. Conformación del tribunal y resolución de recursos

Del relevamiento surge que en 20 audiencias se encontraban presentes solo 2 jueces, sin que en ninguna ocasión las partes objetaran la conformación. Del total de estas audiencias, solo una requirió la intervención del tercer juez que deliberó luego de escuchar el audio. En contraposición,

(37) En la audiencia, el apelante intentó introducir temas de competencia que no estaban señalados en su escrito de presentación, y los jueces lo interrumpieron para decirle que no se extienda más allá del agravio concreto manifestado previamente.

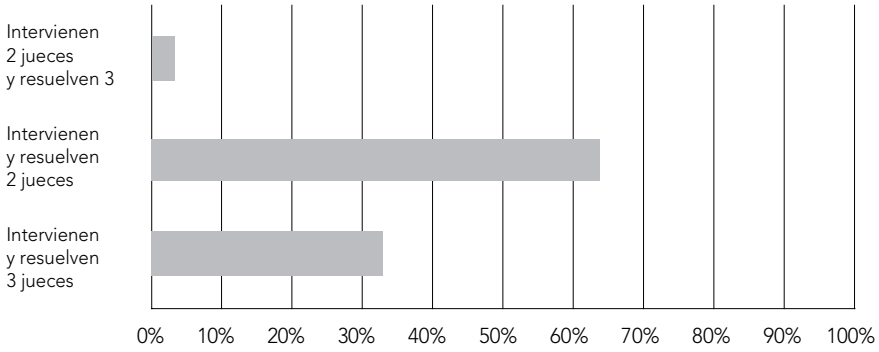
(38) "Rafael" 5/2/2009, nº 35.331, la Sala I.

10 audiencias fueron llevadas a cabo con la presencia de los 3 jueces que conformaban el tribunal.[39]

En cuanto a la resolución de los recursos, 19 fueron resueltos por 2 jueces; es decir, que no existía disidencia que impidiera conformar la mayoría. Solo 11 de los recursos fueron resueltos por 3 jueces, incluyendo aquí la mencionada escucha del audio del párrafo anterior.[40]

En el siguiente cuadro, se detallan los porcentajes totales de audiencias que permiten reflejar la intervención de jueces y resolución de recursos en conjunto, además de distinguir la única excepción en la cual intervienen 2 jueces en la audiencia y resuelven finalmente 3.[41]

GRÁFICO 4. INTERVENCIÓN Y RESOLUCIÓN DE RECURSOS



Intervención y resolución de recursos: Intervienen 2 jueces y resuelven 3 jueces: 3% (1 audiencia). Intervienen y resuelven 2 jueces: 64% (19 audiencias). Intervienen y resuelven 3 jueces 33% (10 audiencias).

A pesar de que en 20 de las 30 audiencias el tribunal se conformó por 2 jueces, se debe acentuar que no todas las Salas comunicaron el motivo de la ausencia del tercer juez ni daban oportunidad a las partes para que

(39) Porcentajes de intervención por el total de 30 audiencias: en el 67% de las audiencias intervienen 2 jueces. En el restante 33%, intervienen 3 jueces.

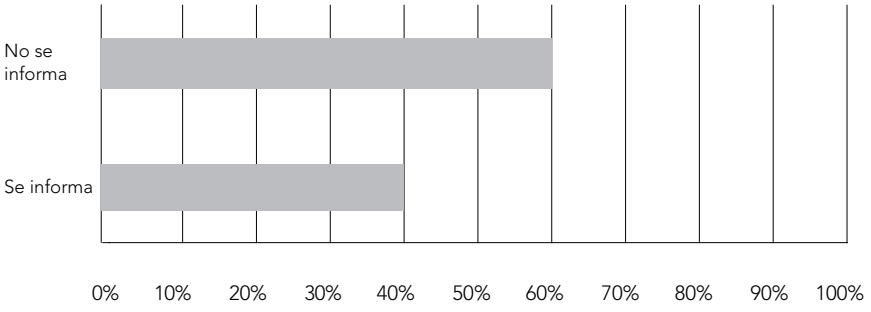
(40) Porcentajes de resolución por el total de 30 audiencias: el 63% de los recursos fue resuelto por 2 jueces. Solo el 37% fue resuelto por 3 jueces.

(41) Los porcentajes anteriores analizan por separado la presencia de jueces y resolución de recursos. En el cuadro, por el contrario, se reflejan los porcentajes de datos cruzados entre presencia de jueces y resolución de recursos.

objeten la conformación. Tampoco advertían a las partes sobre la posibilidad de que intervenga un tercer un juez en caso de que sea necesario, ni daban los nombres de los posibles intervinientes. Quizás esto puede ser consecuencia de que los representantes del Ministerio Público de la Defensa y del Ministerio Público Fiscal ante la Cámara son continuamente los mismos, producto del sistema reflejo del Ministerio Público respecto de la estructura del Poder Judicial. Por lo que se podía percibir, las partes ya conocían la conformación de la Sala y los motivos de la ausencia.

No obstante, es sumamente relevante que los jueces informen a las partes sobre quién será el que intervendrá en caso de no llegar a un acuerdo. Más allá de que el reglamento estime que será el tercer juez o el presidente de la cámara (según el caso), la mención de ello hace a la transparencia del sistema de justicia y permite que las partes puedan conocer quién será el encargado de juzgar y tomar la decisión. No solo asisten defensores públicos o fiscales, también forman parte de las audiencias los abogados particulares y querellantes que, al igual que el resto, deben saber quién tomará la decisión judicial. Solo en el 40% de las audiencias los jueces informaron sobre la identidad del juez que deliberaría en caso de no llegar a un acuerdo.

GRÁFICO 5. INFORMACIÓN A LAS PARTES SOBRE QUIÉN INTENVENDRÁ EN CASO DE DISIDENCIA COMO TERCER JUEZ



Información a las partes sobre quién intervendrá como tercer juez en caso de disidencia: No se informa: 60% (12 audiencias). Se informa: 40% (8 audiencias).

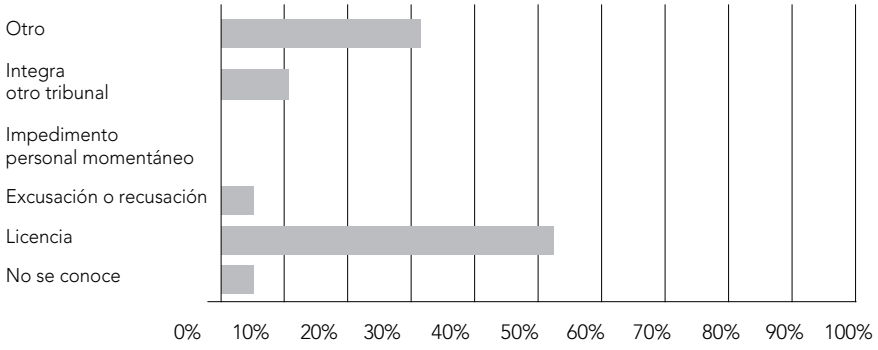
Los motivos de ausencias de los magistrados eran informados al comienzo de la audiencia por el secretario o secretaria a cargo del desarrollo de la misma. En forma mayoritaria, se puede verificar que el motivo principal de ausencias es el goce de licencias. Para el relevamiento se utilizó la información brindada en la audiencia. Es decir, que no se tomó en cuenta

la información ofrecida por los operadores de justicia una vez finalizada la misma. En una de las Salas se encontraban presentes solo 2 jueces porque el tercero estaba visitando una unidad carcelaria.(42) Este dato se corresponde con el 30% de las audiencias cuyo motivo de ausencia se enrola en la categoría "otro".(43) Particularmente en una sala, un juez se encontraba recusado por el fiscal interviniente además de estar de licencia y, a su vez, otro de los jueces que conforma la Sala se encontraba de licencia. Por lo que, el tribunal estaba constituido por un juez de la propia Sala, y otro juez que fue convocado por ejercer funciones en otro tribunal.

En este caso, se pudo conocer la recusación de uno de los jueces en una de las audiencias en presencia del fiscal que lo recusó. En el resto de las audiencias que fueron llevadas a cabo con el mismo fiscal, se mencionaba solo la licencia de los jueces.

En el 5% de los casos no se pudo saber —a través de la audiencia— el motivo por el cual se encontraba ausente el juez y en el 10% de las audiencias el juez tuvo que retirarse para integrar otra Sala en la misma Cámara.

GRÁFICO 6. MOTIVOS DE AUSENCIA DEL TERCER JUEZ



Motivos de ausencia del tercer juez: Otro: 30% (6 audiencias). Integra otro tribunal: 10% (2 audiencias). Impedimento personal momentáneo: 0%. Excusación o recusación: 5% (1 audiencia). Licencia: 50% (10 audiencias). No se conoce: 5% (1 audiencia).

(42) El Protocolo de Relevamiento de las Unidades Carcelarias fue aprobado por Acuerdo General el 7 de diciembre de 2012 y establece que los jueces deberán realizar visitas a las cárceles para el control y seguimiento de las condiciones de detención. Cada Sala tiene designada una Unidad Carcelaria específica.

(43) Ver gráfico 6: Motivos de ausencia del tercer juez.

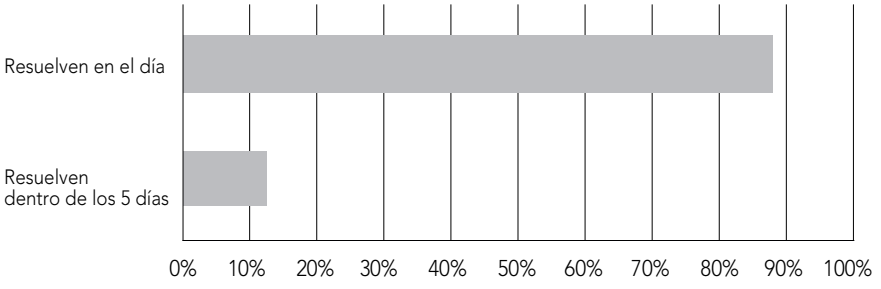
4.2.6. Resolución de los recursos: tiempo y forma

Las Salas organizan su trabajo de manera particular, y cada una de ellas tiene modos disímiles en la forma de deliberar y de comunicar lo resuelto en los recursos. En referencia a la deliberación solo una de las Salas se retira a decidir a un salón contiguo a la sala de audiencias y brinda la resolución a las partes al momento de volver.(44) Es decir, que la decisión es comunicada en forma verbal a las partes al momento de finalizar la audiencia. Dentro de las 6 audiencias observadas en esta Sala, solo en una se hizo alusión al art. 455 CPPN que concede cinco días para deliberar en casos complejos. Por lo que, en ese caso, no se dio a conocer la decisión en el día.

El resto de las Salas, hace salir a las partes de la sala de audiencias, y no comunica en forma verbal la resolución, sino que por el contrario la notifica por cédula. En estos casos, los jueces no hicieron referencia al art. 455 CPPN por lo que, en principio, se daba a entender que resolverían ese mismo día más allá del método de comunicación de la decisión. Pero ello, no siempre sucedió. Aunque luego de ver las resoluciones, la mayoría de los recursos habían sido resueltos en el día por tratarse de casos con personas privadas de la libertad, también hubo apelaciones resueltas en los días posteriores a la audiencia y de ello nada se dijo a las partes.

En su mayoría, los recursos que se resuelven en el día son aquellos en los cuales hay personas detenidas. Los escritos que resuelven los recursos poseen los fundamentos en los cuales se basó la decisión. Nunca se otorgaron los fundamentos en forma oral.

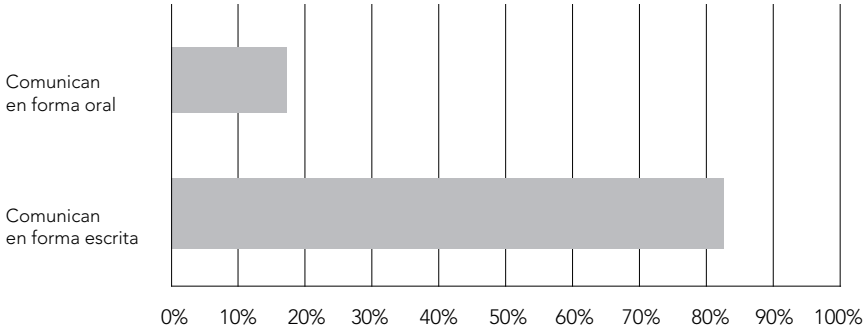
GRÁFICO 7. TIEMPO DE RESOLUCIÓN DE LOS RECURSOS



Tiempo de resolución de los recursos: Resuelven en el día: 87% (26 audiencias.) Resuelven dentro de los 5 días: 13% (4 audiencias).

(44) Sala 1 de la Cámara del Crimen.

GRÁFICO 8. MODO DE COMUNICACIÓN DE LA RESOLUCIÓN DEL RECURSO



Modo de comunicación de la resolución del recurso: Comunican en forma oral 17% (5 audiencias). Comunican en forma escrita 83% (25 audiencias).

4.2.7. El que nunca falta: el expediente

Las audiencias fueron distintas entre sí. En algunas de ellas, se pudieron entrever ciertos rasgos propios de las audiencias previas al juicio conforme a un sistema acusatorio. Otras, por el contrario, se desarrollaron sin contradicción, sin inmediación y hasta incluso sin oralidad como en el caso del apelante que se remitió al escrito de presentación. Sin embargo, y a pesar de que cada Sala organizaba el trabajo a su modo, algo siempre estuvo presente: el expediente.

Además de la minuta que fue mencionada en un comienzo, los jueces solían leer, revisar y remitirse al expediente en cada una de las audiencias. En este marco, los defensores, fiscales y querellantes lo utilizaban a modo de "machete" para recordar los datos que en ese momento no recordaban. Se ha visto, por ejemplo, que al momento de hablar de las personas imputadas, se revisaba el expediente y que, a su vez, era leído por los propios jueces cuando las partes emitían sus alegatos.

La lógica del sistema procesal penal actual demuestra que puede no estar presente en una audiencia la contraparte que resiste el recurso y que puede no estar presente el propio juez que decide. No obstante, también demuestra que en el 100% de las audiencias el que nunca falta es este instrumento formalizado sobre el cual gira y se desarrolla el proceso. La esquizofrenia del procedimiento penal, no logra evadir el expediente que se halla en las salas de audiencias antes que las propias partes.

5 | Conclusiones finales

La Cámara del Crimen cumple con el objetivo que motivó la sanción de la ley: la agilidad en la resolución de los recursos de apelación. Hoy en día, este tribunal resuelve las impugnaciones en el plazo de un mes, lo cual disminuye en gran proporción la dilación indebida del proceso penal. La celeridad es una las características propias de los sistemas modernos de justicia y el trabajo que realiza la Cámara en ese sentido es sumamente eficiente.

Resta señalar que la celeridad debe ser acompañada de un modelo de justicia de calidad, el cual solo se logrará a partir de una reforma total del proceso penal federal. Es inminente la necesidad de implementar un sistema de audiencias desde el inicio de la investigación penal para alcanzar la transparencia en la administración de justicia. A partir de esta reforma integral, se podrán superar las trabas jurisdiccionales y administrativas que actualmente existen en el desarrollo de estas audiencias y en el proceso en general.

Sin embargo, y para seguir avanzando en el cumplimiento de esta reforma parcial dentro del ámbito de la Cámara Nacional de Apelaciones en lo Criminal y Correccional de la Ciudad de Buenos Aires, se proponen algunos cambios que están al alcance de los operadores de justicia en el marco del sistema mixto:

a. Crear la oficina judicial que establece la ley para que lleve las riendas del trabajo administrativo del tribunal y maneje en forma ordenada la agenda de los jueces y la organización total de las audiencias;

b. organizar mediante una acordada un sistema de pool de jueces para cubrir las ausencias en la conformación de las Salas y evitar que los recursos se resuelvan con dos jueces o mediante la escucha del audio;

c. coordinar con el Ministerio Público las acciones necesarias para que las partes asistan a las audiencias independientemente de quién haya interpuesto el recurso;

d. impulsar capacitaciones para los operadores de justicia en materia de litigación;

e. crear carteleras que den publicidad a las audiencias que se desarrollarán en el día para que los ciudadanos que así lo deseen puedan presenciarlas; y,

f. promover la comunicación de la resolución de los recursos en forma oral una vez finalizada la audiencia en todas las Salas, salvo en las circunstancias previstas por ley.

Pues, más allá de que deban mejorarse determinadas cuestiones, la labor cotidiana de este tribunal debe servir de ejemplo para las restantes Cámaras que niegan la posibilidad de utilizar las audiencias orales para resolver las apelaciones. En este sentido, para evitar el incumplimiento de la normativa vigente, se debe hacer hincapié en la importancia de incorporar la gestión judicial en el proceso de implementación de cualquier reforma para que los obstáculos administrativos no cobren gran relevancia cuando las nuevas prácticas choquen con los viejos modismos burocráticos. Retomando a Binder, "no podemos dejar libradas, grandes instituciones con un enorme valor social y político, como es la audiencia oral y pública, a la desorganización, la desidia burocrática o el abandono en manos de los operadores".(45)

Por último, vale destacar esta reforma parcial, a pesar de las complicaciones que acarrean los cambios módicos, para demostrar los beneficios que generan las audiencias tanto para los operadores de justicia como para las personas que se ven involucradas en el proceso penal. Por ello, es hora de empezar a hablar en serio sobre decisiones de calidad, de abandono del trámite y del expediente. Es hora de empezar a ver que las decisiones que se toman en un proceso penal no recaen sobre papeles sino sobre cada uno de nosotros.

(45) Binder, Alberto, "Elogio de la audiencia oral", material de lectura otorgado por el Centro de Estudios de Justicia de las Américas (CEJA) en el marco del Programa Argentino de Capacitación para la Implementación de la Reforma Procesal Penal, 2013.

La oralidad en la etapa recursiva del proceso penal chileno

Las audiencias ante la Corte de Apelaciones de Santiago[1]

por **LEONEL GONZÁLEZ POSTIGO**[2]

I | Introducción

Un aspecto central de los procesos de reforma de la justicia penal experimentados en los últimos veinticinco años en América Latina ha consistido en la reformulación de los sistemas de control de las decisiones judiciales. Sobre el particular, el principal desafío ha residido en abandonar la lógica del recurso como instrumento de control jerárquico propio de la administración colonial de la cual era originario.

En efecto, los nuevos procesos penales adversariales de la región avanzaron hacia la configuración de esquemas recursivos que fuesen compatibles con el nuevo paradigma de enjuiciamiento, en tanto se estructuren sobre la base del resguardo del juicio oral como la etapa central de realización de las garantías del debido proceso.

(1) El presente trabajo se circunscribe en la pasantía de investigación realizada durante el mes de enero del 2013 en el Centro de Estudios de Justicia de las Américas (CEJA), Santiago, Chile.

(2) Investigador del Instituto de Estudios Comparados en Ciencias Penales y Sociales (INECIP).

Sin embargo, lo cierto es que la implementación de estos nuevos diseños no fue uniforme en los países de Latinoamérica.(3) En algunos de ellos, si bien se instaló un sistema de audiencias orales para adoptar las decisiones de la etapa preparatoria y del juicio, políticamente se optó por mantener un modelo de recursos formal-escrito. Al mismo tiempo, otros Estados, como la República de Chile, se inclinaron por establecer la oralidad para la actividad recursiva, disponiendo expresamente que la vista de los recursos tuviera que realizarse en el marco de una audiencia pública.

En este trabajo se analizará el sistema de impugnaciones consagrado a partir de la reforma al proceso penal chileno, desde una perspectiva de diseño normativo, pero fundamentalmente de desempeño práctico respecto al modo en que funciona en la actualidad la Corte de Apelaciones de Santiago. Para finalizar, se pondrán de resalto los beneficios que posee la oralidad por sobre la escrituración en el régimen de los recursos.

2 | El proceso penal y su reforma en Chile: impacto en la configuración de las vías de impugnación

2.1 | Antecedentes y lineamientos básicos de la reforma

La historia de la legislación procesal penal chilena se caracteriza por poseer una incuestionable base común: la notable influencia ejercida por España durante la época de la colonia al haber instaurado un ordenamiento de corte netamente inquisitivo.

Este sistema continuó vigente en lo fundamental con el transcurso del tiempo, incluso tras el surgimiento de la nueva república a principios del siglo XIX, hasta el dictado de un renovado código de procedimiento penal

(3) Al respecto, véase el informe "Los regímenes recursivos en los sistemas procesales penales acusatorios en las Américas: Aspectos centrales", [en línea] www.cejamericas.org. Contiene reportes específicos que describen el sistema de recursos en contra de las sentencias definitivas penales en algunos países de la región.

en el año 1906.[4] Si bien se trataba de un cuerpo legislativo totalmente nuevo, lo cierto es que éste código mantuvo incólume las estructuras básicas heredadas del período colonial del que provenían.[5]

La primera instancia de este proceso se dividía en dos etapas: el sumario y el plenario. La fase de investigación o instrucción —sumario— se desarrollaba de manera secreta y bajo una intensa delegación de funciones en los operadores subalternos, la policía y demás auxiliares, mientras que el juicio penal —plenario— suponía el primer momento en el cual las partes podían realizar un auténtico debate ante el juez, el cual estaba revestido —en principio— con los caracteres de publicidad y contradicción.

La figura central de este sistema era el juez del crimen, a quien se le atribuían las facultades de investigación, acusación y fallo. Junto con las funciones jurisdiccionales, este juez asumía las tareas administrativas de organización del tribunal que estaba a su cargo, contando para ello con más de diez funcionarios.

Por otro lado, el trabajo de segunda instancia le correspondía a las Cortes de Apelaciones, que ejercían jurisdicción sobre el territorio en el que funcionaba el respectivo tribunal de primera instancia y se organizaban en salas no especializadas integradas por tres jueces profesionales. En suma, existían 17 Cortes de Apelaciones en todo el país. La Corte Suprema de Justicia también actuaba en materia penal, toda vez que su competencia correspondía al control de casación y al control disciplinario ejercido por vía del conocimiento del recurso de queja.

Como se advierte, el modelo procesal inquisitorial siguió rigiendo en Chile durante el siglo XX, habiéndose fortalecido en atención a determinados

(4) Para una explicación de los aspectos centrales del modelo procesal penal instaurado en 1906, véase Duce, Mauricio y Riego, Cristián, "La reforma procesal penal en Chile. Informe acerca del proceso de reforma al sistema de enjuiciamiento criminal chileno", en *Sistema Acusatorio, Proceso Penal, Juicio Oral en América Latina y Alemania*, Caracas, Fundación Konrad Adenauer, 1995, p. 145 y ss.

(5) De ello dan cuenta las principales fuentes en las cuales se sustenta, entre las que se destacan: la legislación colonial española que se aplicó hasta su entrada en vigencia, como por ejemplo, las Siete Partidas; las leyes de enjuiciamiento criminal españolas de 1852 y 1882, y algunas normas jurídicas nacionales contenidas tanto en la carta constitucional de 1833 como en las leyes de garantías constitucionales de 1884 y 1891. Duce, Mauricio y Riego, Cristian, *La reforma procesal...*, *op. cit.*, p. 51.

cambios que operaron a su favor. Uno de ellos, probablemente el de mayor importancia, consistió en la supresión de los promotores fiscales en primera instancia, a comienzos de 1927.[6] Ésta medida tendió a que se concentren las facultades de investigación y juzgamiento en poder del mismo funcionario judicial, quien tenía a su cargo la actuación en la parte principal, como acusador o denunciante, procediendo de oficio.[7]

Ahora bien, en las décadas posteriores se comenzaron a plantear una serie de propuestas que fueron denotando cierta preocupación por el funcionamiento del sistema de justicia penal, entre las que pueden mencionarse la separación de las funciones entre jueces instructores y sentenciadores, el restablecimiento de la figura del Ministerio Público, la creación de un Consejo Nacional de la Magistratura y de una escuela judicial, y la modificación de las formas de acceso y promoción en la carrera judicial entre otras aspiraciones de menor impacto.

A fines de la última década del siglo XX, se comenzaron a materializar los esfuerzos por readecuar la administración de justicia chilena a los requerimientos propios de un Estado democrático de Derecho, en el marco de los movimientos de reforma procesal que comenzaron a suceder en América Latina. Es así que la transformación real del sistema de justicia penal en Chile se inició formalmente a partir de la presentación en el Congreso Nacional del proyecto de ley de un nuevo Código Procesal Penal, en el mes

(6) "En los casos en que durante la primera instancia se exija o se autorice el simple dictamen o audiencia o citación del Ministerio Público, se prescindirá de este trámite. En todos los casos en que las leyes determinen la intervención del Promotor Fiscal como parte principal, como acusador público o como denunciante, el Juzgado procederá de oficio" (decreto-ley 426, 03/03/1927).

(7) El desplazamiento del Ministerio Público Fiscal hacia un papel secundario se produjo con mucha fuerza en América Latina con anterioridad a los procesos de reforma. Respecto al caso chileno, Maier sostiene que "se trata de un ejemplo de falta de hipocresía, pues en los demás países conservadores del procedimiento penal colonial, en los cuales imperó el procedimiento registrado, el juez unipersonal, idéntico para la instrucción y el juzgamiento, con facultades omnímodas para proceder de oficio, el papel del ministerio público, oficio existente, representa tan sólo una formalidad sin contenido material alguno, que persigue el fin exclusivo de crear una imagen necesaria en el sistema judicial actual, en materia penal, para evitar un juicio de censura abierto sobre su sistema de realización del Derecho penal: modernamente, la falta de ministerio público, la carencia de una fiscalía, y la atribución directa de su tarea a un juez —que, además, juzga— torna extremamente visible para el observador la raíz ideológica del procedimiento penal vigente y la falta de garantías que el procedimiento penal —se supone— debe tener en un Estado de Derecho". Véase Maier, Julio, *Derecho Procesal Penal*, t. II, Bs. As., del Puerto, 2004, p. 318.

de junio de 1995, el cual tomó entre sus fuentes al código modelo para Iberoamérica en conjunto con diversos textos de legislación extranjera.

Finalmente, tras un trabajo largo y complejo, este proyecto fue sancionado a finales del año 2000 e implementado de manera progresiva en cada una de las regiones del país, concluyendo en junio del 2005 con el ingreso del nuevo sistema en la Región Metropolitana, que contiene a la ciudad de Santiago.

El nuevo ordenamiento consagró un proceso penal con rasgos marcadamente acusatorios, aparejando reformas en los tribunales que abarcaron tanto las funciones jurisdiccionales, al crearse dos nuevas categorías de jueces, como las de administración, donde se estableció todo un nuevo sistema de gestión por el cual se suprimió el despacho tradicional y se reemplazó por despachos colectivos, que abarcan a todos los jueces de una categoría dentro de cada ciudad, y cuya administración se entrega a un equipo profesional especializado.[8]

En relación con las características centrales de la reforma chilena, el nuevo sistema introdujo dos cambios fundamentales: por una parte, estableció la separación entre las funciones de acusación y juzgamiento, suprimiendo la figura del juez de instrucción y entregando la tarea de preparación del juicio al Ministerio Público supervisado por un juez especialmente diseñado a tal fin: el juez de garantías. Por otro lado, el nuevo esquema consagró al juicio oral como el elemento rector del conjunto del proceso. Esta centralidad del juicio implicó que la etapa de investigación se convirtiera en una fase estrictamente preparatoria, toda vez que los antecedentes recopilados en ella solo tendrían valor al momento en que se presenten en la audiencia de juicio bajo las reglas del contradictorio.

2.2 | Breve descripción del sistema recursivo vigente con anterioridad al nuevo modelo

El régimen de recursos establecido en el código de procedimiento penal del año 1906 funcionaba sobre la base de un agudo sistema de controles verticales, al punto que todas las decisiones adoptadas por el juez del

(8) CEJA, *Reformas procesales penales en América Latina: Resultados del Proyecto de Seguimiento*, Santiago de Chile, CEJA, 2005, p. 31 y ss.

crimen eran objeto de revisión por los tribunales superiores, incluso sin reclamación de parte.

El procedimiento ante las Cortes de Apelaciones se efectuaba en el marco de una audiencia en la cual los jueces tomaban conocimiento de los hechos a partir de un resumen oral llamado "relación", históricamente realizado en forma secreta por un funcionario judicial denominado "relator", tras lo cual las partes alegaban verbalmente sus peticiones concretas.

Los mecanismos impugnativos centrales que proveía la norma eran los recursos de apelación, de casación, y la consulta. Esta última resultaba paradigmática en tanto permitía ejercer un amplio control sobre la mayoría de los casos, ya que no solo procedía contra las sentencias definitivas no apeladas, sino que también en relación a un conjunto de resoluciones tales como los sobreseimientos, o las que se emitían sobre la libertad provisional de los procesados.(9)

Sobre su regulación, del antiguo código disponía:

> "Las sentencias definitivas de primera instancia que no fueren revisadas por el respectivo tribunal de alzada por la vía de la apelación, lo serán por la vía de la consulta en los casos siguientes: 1) Cuando la sentencia imponga pena de mas de un año de presidio, reclusión, confinamiento, estrañamiento o destierro, o alguna otra superior a éstas; 2) Cuando el proceso versare sobre delito a que la ley señale pena aflictiva" (art. 568),(10)

con lo cual se observa que prácticamente todas las decisiones adoptadas por el juez del crimen eran plausibles de ser revisadas por medio de la consulta.

Con relación a este sistema, se ha explicado que

> "el origen de esta fuerte tendencia al sometimiento de los asuntos por el tribunal superior se encuentra precisamente en la con-

(9) De hecho, Duce y Riego señalan que en el año 1995, el 48% de los ingresos a la Corte de Apelaciones de Santiago estaba constituido por las consultas. Duce, Mauricio y Riego, Cristian, *La reforma procesal...*, *op. cit.*, p. 158.

(10) CPP chileno, 1906, [en línea] www.leychile.cl

> vicción de los redactores del código de la necesidad de imponer controles a la actividad del juez de primera instancia, cuyas funciones concentradas les hacían dudar de la suficiente garantía de imparcialidad".(11)

En rigor, tanto el recurso de apelación como la consulta no estaban diseñados para suplir las deficiencias de garantías de la primera instancia, en razón de que el conocimiento que los jueces de los tribunales superiores tenían sobre el proceso era estrictamente para ejercer un control de la actividad jurisdiccional realizada por los estamentos judiciales inferiores. A su vez, el sistema de la doble instancia se constituía como un elemento que acrecentaba la poca autonomía de los tribunales de inferior rango, pues el papel que estos últimos desempeñaban estaba subordinado a los parámetros básicos de la Corte de Apelaciones de la cual dependían.

2.3 | La instalación del sistema adversarial: aspectos centrales del régimen de recursos

En relación al sistema de control de las decisiones judiciales, el nuevo proceso penal provocó una transformación radical del modelo que estaba vigente. A este respecto, es posible identificar tres ejes representativos sobre los cuales se asentó el cambio.

El primero de ellos dice relación con la disminución de la intensidad del régimen de recursos, en atención a la desaparición de la vía de la consulta. Ésta medida implicó que las posibilidades de impugnación se constituyan en función del surgimiento de un agravio concreto, y que la legitimación para ello esté solamente en poder de los intervinientes en la contienda, esto es, la imposibilidad de que sean los propios jueces quienes mecanicen la revisión de oficio de las resoluciones jurisdiccionales.

Un segundo aspecto característico del nuevo esquema recursivo se vinculó con la eliminación del sistema de la doble instancia, según el cual se autorizaba a que un tribunal superior realice un nuevo examen sobre los hechos fijados en el juicio, en punto a la amplitud que confería el recurso

(11) Riego, Cristian, *Aproximación a una evaluación del proceso penal chileno, en Reformas procesales en América Latina*, Santiago de Chile, Corporación de Promoción Universitaria, 1993, p. 266.

de apelación. Los límites del nuevo régimen se vincularon con una restrictiva extensión para impugnar las sentencias dictadas tras la celebración de un debate oral.

El ámbito de la apelación quedó circunscrito a las resoluciones más relevantes adoptadas durante la investigación por el juez de garantías, mientras que se estableció el recurso de nulidad como la vía procedente para cuestionar las sentencias definitivas, en base a causales específicas que habilitan su interposición, gobernadas por el principio de la intangibilidad de los hechos acreditados en el juicio.

La contradicción existente entre la apelación y los principios de oralidad e inmediación fue evidenciada durante la tramitación legislativa del proyecto en la Cámara de Diputados, acerca de lo cual se dijo que

> "la oralidad del procedimiento requiere que el tribunal que conoce el juicio tenga el máximo poder de decisión. Si en vez de darle el poder de decisión final al tribunal que asiste al juicio oral se le otorga a otro tribunal, que conocerá de la causa por la vía de la lectura del expediente, se estaría poniendo el centro del debate en la lectura del expediente y no en el juicio oral".(12)

Esto se traduce en que la apelación no se correspondía con la lógica establecida en el nuevo código, en tanto se confiere centralidad al debate público y contradictorio, lo cual supone que los principales controles del proceso sean aquellos que se den al interior del juicio como producto de la intervención simultánea de todos los intervinientes (modelo de controles horizontales), quienes se encuentran en una misma franja jerárquica por medio de la que se limitan mutuamente.

De hecho, esta concepción fue enunciada expresamente en el mensaje enviado por el Poder Ejecutivo chileno en el proyecto de ley del Código Procesal Penal, a saber:

> "Los cambios más importantes que el proyecto propone se refieren a la apelación y a la consulta. Estos mecanismos de control no resultan en general compatibles con el nuevo sistema.

(12) Horvitz Lennon, María Inés y López Masle, Julián, *Derecho Procesal Penal chileno*, t. II, Santiago de Chile, Editorial Jurídica de Chile, 2002, p. 355.

> La primera razón para ello dice relación con la contradicción entre la forma de tramitación de esos recursos y la centralidad del juicio oral en el procedimiento propuesto. La vigencia de un sistema oral requiere que el fundamento fáctico de la sentencia provenga de la apreciación directa de las pruebas que los jueces obtienen en el juicio. En consecuencia, su revisión por parte de jueces que no han asistido al juicio y que toman conocimiento de él por medio de actas, lo priva de su centralidad confiriéndosela, en cambio, a la tramitación del recurso de apelación".(13)

De lo expuesto, se advierte que la intención inicial —plasmada con posterioridad en el texto normativo— consistió en establecer un régimen de recursos muy limitado en contra de las sentencias que sean producto de un juicio oral. Sobre esta base, se ha afirmado que

> "para que el juicio cumpla su función se requiere que las decisiones se tomen sobre la base de la prueba que en él se presente y sobre la base de los debates que en él tengan lugar. Si con posterioridad al juicio las decisiones pueden ser revisadas y modificadas por un tribunal superior que no asistió a la audiencia, entonces todo el sentido del debate se desvirtúa, porque las partes y cualquier interesado entienden claramente que lo central no es lo que ocurre en el juicio, ni la prueba presentada en él, sino que las actas del mismo y su posterior lectura por el tribunal será la base de la decisión que ha de resolver en definitiva el caso".(14)

En tercer lugar, como consecuencia de la supresión de la doble instancia, el nuevo sistema de impugnaciones estableció la necesidad de que se produzca una doble conformidad judicial a los fines de operativizar una sentencia condenatoria. Esto significa que el nuevo código ha cambiado substancialmente la lógica recursiva contra la sentencia de juicio, tanto que ahora se le ha reconocido al imputado una garantía judicial mínima de exigir al Estado que dos órganos jurisdiccionales se expresen de forma concordante respecto al dictado de una condena en su contra.

(13) "Mensaje del Poder Ejecutivo" en *Código Procesal Penal*, Santiago de Chile, Editorial Jurídica de Chile, 2012, p. 40.

(14) Duce, Mauricio y Riego, Cristian, *La reforma procesal...*, *op. cit.*, p. 506.

Sobre el particular, se ha sostenido que

> "habiéndose concebido en primera instancia un tribunal colegiado integrado por tres miembros, cuyas decisiones son impugnables a través del recurso de nulidad, y habiéndose estructurado este último como un recurso desformalizado, que permite controlar (…) el respeto a los derechos y garantías comprometidos en el procedimiento penal y la conformidad de la sentencia con las reglas de la sana crítica, la posibilidad de apelación habría resultado del todo superflua. Lo que resulta realmente trascendente desde el punto de vista del derecho al recurso no es la doble instancia, sino la doble conformidad".(15)

En definitiva, el nuevo sistema de impugnaciones consagra el recurso de apelación contra toda resolución adoptada por los jueces de garantías en la etapa preparatoria, mientras que establece un recurso de nulidad, con notorias limitaciones, contra las sentencias adoptadas tras la celebración del juicio oral.

(15) Horvitz Lennon, María Inés y López Masle, Julián, *Derecho Procesal Penal…*, *op. cit.*, p. 358. En nuestro país, en la actualidad, se continúa sosteniendo que la garantía del doble conforme exige la revisión de las sentencias por parte de un tribunal orgánicamente superior a aquel del que emana la resolución impugnada: "en cuanto al órgano del recurso, creemos que los requisitos exigidos para el mismo se satisfacen con el establecimiento en las respectivas jurisdicciones de un órgano jurisdiccional distinto y jerárquicamente superior al tribunal emisor del fallo impugnado" (Salido, María Belén, "La vigencia de la garantía del "doble conforme" en el proceso penal: una tarea pendiente, un derecho no suficientemente escuchado aún", en *Libro de Ponencias del XXVII Congreso Nacional de Derecho Procesal*, Córdoba, 2013). Sin embargo, hace muchos años, Alberto Binder sostuvo con claridad que el sujeto condenado tiene la facultad de exigir la revisión de su condena por un juez o tribunal superior, sin considerar a éste último en términos jerárquicos, sino materiales, al afirmar que "la interpretación correcta es la que indica que el derecho fundamental consiste en la facultad de desencadenar un mecanismo real y serio de control del fallo, por un funcionario distinto del que lo dictó y dotado de poder para revisar el fallo anterior, es decir, que su revisión no sea meramente declarativa, sino que tenga efectos sustanciales sobre el fallo" (Binder, Alberto, *Introducción al Derecho Procesal Penal*, Bs. As., Ad-Hoc, 1993, p. 265). Incluso, recientemente, la Procuradora General de la Nación ha afirmado que "la referencia a que el derecho a recurrir el fallo condenatorio se ejerce ante 'un juez o tribunal superior'debe entenderse como la exigencia de que el órgano revisor pueda brindar garantías de independencia e imparcialidad suficientes para asegurar la satisfacción del fin al que apunta la regla del art. 8.2.h de la Convención, y no como una obligación de asegurar la existencia de una estructura de tribunales organizados jerárquicamente" (Procuradora General de la Nación, dictamen D. 429. XLVIII., D. Felicia s/ Recurso de casación, 04/10/2013).

2.3.1. Aproximación general al marco normativo vigente

El sistema de impugnaciones chileno se encuentra regulado en el libro tercero del CPPChile, entre los arts. 352 y 387, por medio del cual se establecen las normas relativas a los recursos de reposición, apelación y nulidad.

La regla general a todos ellos dispone que la vista de las causas se efectúe en una audiencia pública, iniciándose con el otorgamiento de la palabra a la parte recurrente para que exponga sus fundamentos, con la posterior intervención de los recurridos a fin de que formulen aclaraciones respecto de los hechos o de los argumentos vertidos en el debate. En cualquier momento de la audiencia, los miembros del tribunal podrán formular preguntas a los representantes de las partes o pedirles que profundicen su argumentación o la refieran a algún aspecto específico de la cuestión debatida. Concluido el debate, el tribunal pronunciará sentencia de inmediato o, de lo contrario, establecerá una fecha a esos efectos (art. 358).

Ingresando al análisis de cada recurso en particular, el nuevo ordenamiento regula que la reposición procede contra las sentencias interlocutorias, los autos y los decretos dictados fuera de las audiencias (art. 362), como así también en contra de las resoluciones pronunciadas durante el transcurso de las mismas (art. 363). En ambos casos, con esta vía se pretende que el mismo tribunal que adoptó la decisión sea quien la revise, y resuelva su eventual revocación o modificación.

Respecto al recurso de apelación, en línea con el criterio expuesto en el acápite anterior, el código dispone manifiestamente que sean inapelables las resoluciones dictadas por un tribunal de juicio oral en lo penal (art. 364). Con lo cual, reduce su procedencia a lo resuelto por el juez de garantías en el transcurso de la investigación penal preparatoria. En este sentido, el ordenamiento establece que las disposiciones dictadas por el juez de garantía serán apelables en dos casos: a) cuando pusieren término al procedimiento, hicieren imposible su prosecución o la suspendieren por más de treinta días;[16] y b) cuando la ley lo señalare expresamente[17] (art. 370).

(16) No obstante esta regulación, constituyen excepciones a esta regla la sentencia definitiva dictada por el juez de garantía en el procedimiento simplificado (art. 399) y en el procedimiento por delito de acción privada (arts. 405 y 399), respecto de las cuales la apelación se declara expresamente improcedente.

(17) El Código indica expresamente la procedencia de la apelación en contra de resoluciones dictadas por el juez de garantía en los siguientes casos: 1. la resolución que declara inadmisi-

Ahora bien, el recurso central del nuevo sistema es, sin dudas, el de nulidad. Aunque este mecanismo se ha construido sobre la base de la casación, lo cierto es que se ha procurado diseñar una versión superadora del modelo tradicional, con el fin de abandonar los problemas de formalismos que históricamente ha tenido. Es por ello que la nulidad se ha configurado de modo que su procedencia se torne más accesible.

En cuanto a su regulación normativa, el código dispone que éste recurso procede para invalidar el juicio oral y la sentencia definitiva, o solamente ésta, debiendo interponerse ante el tribunal que hubiere conocido del juicio (art. 372), siendo competentes para su conocimiento la Corte de Apelaciones respectiva de la jurisdicción del tribunal apelado y la Corte Suprema de Justicia (art. 376).

Se estipulan dos tipos de causales que dan lugar a la nulidad, que operan con lógicas diferentes: las genéricas y las específicas ("motivos absolutos"). Sobre las primeras, el art. 373 del código establece que procederá la declaración de nulidad:

a. Cuando, en cualquier etapa del procedimiento o en el pronunciamiento de la sentencia, se hubieren infringido sustancialmente derechos o garantías asegurados por la Constitución o por los tratados internacionales ratificados por Chile que se encuentren vigentes, y

b. Cuando, en el pronunciamiento de la sentencia, se hubiere hecho una errónea aplicación del derecho que hubiere influido sustancialmente en lo dispositivo del fallo.

ble la querella (art. 115, inc. 1); 2. la resolución que declara el abandono de la querella (art. 120, inc. final); 3. la resolución que ordena, mantiene, niega lugar o revoca la prisión preventiva, cuando hubiere sido dictada en una audiencia (art. 149); 4. la resolución que ordena, mantiene, niega lugar o revoca una medida cautelar general del art. 155 (art. 155, inc. final y art. 149); 5. la resolución que niega o da lugar a medidas cautelares reales (art. 158); 6. la resolución que se pronuncia acerca de la suspensión condicional del procedimiento (art. 237, inc. 6); 7. la resolución que revoca la suspensión condicional del procedimiento (art. 239); 8. la resolución que decreta el sobreseimiento definitivo por no haber comparecido el fiscal a la audiencia de cierre de la investigación o haberse negado en ésta a declararla cerrada, encontrándose vencido el plazo legal para hacerlo (art. 247); 9. el sobreseimiento temporal y definitivo (art. 253); 10. la resolución que recae en las excepciones de incompetencia, litis pendencia y falta de autorización para proceder criminalmente, opuestas a la acusación como excepciones de previo y especial pronunciamiento (art. 271, inc. 2); 11. el auto de apertura del juicio oral, pero sólo por el ministerio público por la exclusión de pruebas decretada por el juez de garantía de acuerdo a lo previsto en el inciso tercero del art. 276 (art. 277, inc. final); y 12. la sentencia definitiva dictada por el juez de garantía en el procedimiento abreviado (art. 414, CPP). Horvitz Lennon, María Inés y López Masle, Julián, *Derecho Procesal Penal…*, *op. cit.*, p. 372.

Una primera lectura de este artículo podría llevar a la conclusión de que en realidad ambos incisos refieren a un mismo supuesto: la vulneración de derechos consagrados en el texto constitucional o en los instrumentos internacionales. Sin embargo, lo cierto es que responden a conceptos distintos, pues podría decirse que la regla del primer inciso tuvo como sentido principal resaltar a las garantías del debido proceso como el criterio fundamental de validez del procedimiento, lo que por otra parte constituye la columna vertebral del nuevo código;[18] mientras que en el segundo inciso, para acreditar la existencia de una infracción o errónea aplicación de la ley, se requiere un efecto trascendente y concreto, de manera tal que su verificación implique una real variación respecto de lo que racional y jurídicamente debería fallarse y lo que efectivamente se resolvió en la sentencia a impugnar.[19]

En suma, en ambos supuestos se le exige al recurrente un ejercicio argumentativo en relación al modo en que determinados hechos constituyen una infracción en el caso particular, más allá de la lógica subyacente en cada uno de ellos.

Por otra parte, en cuanto a los motivos absolutos de nulidad, el art. 374 del código dispone que el juicio y la sentencia serán siempre anulados:

a. Cuando la sentencia hubiere sido pronunciada por un tribunal incompetente, o no integrado por los jueces designados por la ley; cuando hubiere sido pronunciada por un juez de garantía o con la concurrencia de un juez de tribunal de juicio oral en lo penal legalmente implicado, o cuya recusación estuviere pendiente o hubiere sido declarada por tribunal competente; y cuando hubiere sido acordada por un menor número de votos o pronunciada por menor número de jueces que el requerido por la ley, o con concurrencia de jueces que no hubieren asistido al juicio.

b. Cuando la audiencia del juicio oral hubiere tenido lugar en ausencia de alguna de las personas cuya presencia continuada exigen, bajo sanción de nulidad, los arts. 284 y 286;

c. Cuando al defensor se le hubiere impedido ejercer las facultades que la ley le otorga;

(18) Duce, Mauricio y Riego, Cristian, *La reforma procesal...*, *op. cit.*, p. 517.

(19) Rieutord, Andrés, *El recurso de nulidad en el nuevo proceso penal*, Santiago de Chile, Editorial Jurídica de Chile, 2007, p. 49

d. Cuando en el juicio oral hubieren sido violadas las disposiciones establecidas por la ley sobre publicidad y continuidad del juicio;

e. Cuando, en la sentencia, se hubiere omitido alguno de los requisitos previstos en el art. 342, letras c), d) o e);

f. Cuando la sentencia se hubiere dictado con infracción de lo prescrito en el art. 341, y

g. Cuando la sentencia hubiere sido dictada en oposición a otra sentencia criminal pasada en autoridad de cosa juzgada.

Como puede observarse, se describen situaciones de hecho concretas en la cuales el legislador ha previsto que siempre se genera una infracción susceptible de nulidad. En consecuencia, el trabajo del recurrente basta con probar que en el caso ha ocurrido una de las situaciones de hecho descritas en alguno de los incisos de éste artículo.

No obstante, se ha afirmado que "la redacción de algunas de estas hipótesis no ha cerrado completamente la descripción de hechos que la hace procedente, lo que genera que a propósito de discutir su procedencia se abra el camino para un tipo de argumentación similar a la exigida por el art. 373 a)".(20) Con lo cual, podría decirse que determinados motivos absolutos de nulidad (por ejemplo, los del inciso c y e) son complementarios de las causales genéricas, en atención a que consisten en infracciones a garantías del debido proceso.

Por último, en caso de que éste recurso sea acogido por el tribunal, la regla general es que se dispone un reenvío a fin de que se celebre un nuevo juicio oral, debiendo indicarse con claridad en que estado del proceso se debe retomar su curso, evitando incurrir en el agravio. Empero, el código contempla excepciones por las cuales la Corte podrá invalidar solo la sentencia y dictar, sin nueva audiencia pero separadamente, sentencia de reemplazo, si la causal de nulidad no se refiriere a formalidades del juicio ni a los hechos o circunstancias que se hubieren dado por probados, sino se debiere a que el fallo hubiere calificado de delito un hecho que la ley no considerare tal, aplicado una pena cuando no procediere aplicar pena alguna, o impuesto una superior a la que legalmente correspondiere (art. 385).

(20) Duce, Mauricio y Riego, Cristian, *La reforma procesal...*, *op. cit.*, p. 522.

3 | El funcionamiento de la Corte de Apelaciones de Santiago

Este capítulo estará destinado a la descripción del funcionamiento práctico de la Corte de Apelaciones de Santiago de Chile. En atención a que este tribunal ha instalado un sistema de oralidad para la toma de decisiones en la actividad recursiva, el trabajo de investigación efectuado se estructuró sobre la base de la observación de audiencias y la realización de entrevistas con los operadores del sistema judicial.

Para su abordaje concreto, se han seleccionado una serie de variables metodológicas que dan cuenta de los siguientes aspectos:

a. Diseño institucional
b. Organización administrativa y sustanciación del recurso
c. Dinámica de la audiencia
d. Información estadística sobre los tiempos procesales

Como se observa, en primer lugar se han propiciado atender las cuestiones relativas a la estructura del tribunal, su integración, la infraestructura edilicia, el sistema de registro, y las funciones del personal de las salas.

A su vez, se han escogido parámetros sobre la gestión administrativa de los recursos, en función del criterio por el cual se han distribuido las tareas no jurisdiccionales.

Ahora bien, el eje central del diagnóstico se encuentra focalizado en las cuestiones vinculadas con la dinámica del recurso durante el transcurso de la audiencia, puntualizando de qué modo los litigantes presentan sus agravios, cómo los fundamentan, de qué manera se genera el contradictorio entre los intervinientes, el rol que les cabe a los Ministros durante el debate, la información que se utiliza, y la manera por la cual se adoptan las decisiones judiciales en éste contexto.

Tras todo ello, se presentarán datos estadísticos que operan en distintos niveles: por una parte, los tiempos en que se incurren entre la entrada de los recursos y la fijación de las vistas (gestión administrativa); el plazo que transcurre desde la celebración de la audiencia y la lectura de la resolución

(función jurisdiccional); y la duración total entre el ingreso de la impugnación y su resolución (funcionamiento general de la Corte).

3.1 | Diseño institucional

3.1.1. Cuestión previa: organización del Poder Judicial de Chile

Un aspecto inicial a destacar es que el Poder Judicial de Chile se estructura a partir de una organización vertical, es decir, en función de distintas instancias judiciales.

En el fuero penal consisten en una primera instancia conformada por jueces de garantías para la etapa de investigación, y tribunales de juicio oral en lo penal para la audiencia de debate. La segunda instancia está dada por diecisiete Cortes de Apelaciones distribuidas a lo largo de todo el país, las cuales están integradas por Ministros de corte como así también por dos categorías de personas que eventualmente los reemplazan, llamados "abogados integrantes"[21] y "fiscales judiciales".

Con lo cual, como cuestión previa, no debe soslayarse que si bien el nuevo código de Chile consagró un proceso penal adversarial, lo cierto es que la organización judicial penal continúa siendo vertical, detalle que no será menor a la hora de analizar de qué manera se diseña un régimen recursivo.

En el último escalón se encuentra la Corte Suprema de Justicia de Chile, que es un tribunal colegiado compuesto por veintiún miembros denominados Ministros, uno de los cuales es su Presidente, quien es designado por sus pares, y dura dos años en sus funciones. Los Ministros son designados por el Presidente de la República, quien los elige de una nómina de cinco personas que, en cada caso, propone la Corte Suprema, y con acuerdo del Senado. De los veintiún miembros, dieciséis deben provenir de la carrera judicial, y cinco deberán ser abogados extraños a la administración de justicia, tener por lo menos quince años de título, haberse destacado en la actividad profesional o universitaria, y cumplir los demás requisitos que señale la ley orgánica constitucional respectiva.[22]

(21) Mediante las Actas 273-2008 y 274-2008, ambas del 07/11/2008, la Corte Suprema determinó el procedimiento de formación de ternas para el nombramiento de Abogados Integrantes de las Cortes de Apelaciones del país.

(22) Para mayor información, véase [en línea] http://www.poderjudicial.cl/

3.1.2. Estructura e integración de la Corte de Apelaciones de Santiago

El territorio jurisdiccional de esta Corte comprende la parte de la Región Metropolitana de Santiago correspondiente a las provincias de Chacabuco y de Santiago, con exclusión de las comunas de Lo Espejo, San Miguel, San Joaquín, La Cisterna, San Ramón, La Granja, El Bosque, La Pintana y Pedro Aguirre Cerda.

Se ubica físicamente en el Palacio de los Tribunales de Justicia, en donde también se halla la sede de la Corte Suprema de Justicia, y de la Corte Marcial del Ejército, Fuerza Aérea y Carabineros.

La Corte de Apelaciones de Santiago se encuentra dividida en diez salas conformada cada una de ellas por tres Ministros. En suma, son treinta y un Ministros, de los cuales uno de ellos es elegido anualmente para que ejerza la presidencia del cuerpo.

Los requisitos para ser elegido Ministro de Corte de Apelaciones o fiscal judicial de tribunal de alzada se encuentran estipulados en el Código Orgánico de Tribunales (art. 253). Ellos consisten en ser de nacionalidad chilena, tener título de abogado, haber ejercido el cargo de juez, y haber aprobado el curso de perfeccionamiento que dicta la Academia Judicial. Una vez producida una vacante, los interesados deben presentar sus antecedentes en el concurso público que convoca la Corte Suprema, la cual elabora una terna que es enviada al Poder Ejecutivo a fin de que elijan un candidato y lo designen.

Del total de las salas, en la Corte de Santiago tan solo una de ellas se especializa temáticamente, pues la sala décima resuelve solamente recursos en materia laboral y, excepcionalmente, hace lo propio con causas de la tabla extraordinaria en lo penal. En las nueve restantes, tal como veremos más adelante, se intercalan recursos de diferentes especialidades del área del derecho. Sin embargo, es menester señalar que en el marco de las periódicas jornadas de reflexión que lleva a cabo la Corte Suprema, se ha discutido en el año 2010 la posibilidad de reorganizar las Cortes de Apelaciones de Santiago, Valparaíso, San Miguel y Concepción a partir de salas especializadas.[23] No obstante, hasta la fecha no se han materializado tales propuestas.

(23) En relación a la especialización de las Cortes de Apelaciones, las conclusiones a las cuales arribó la Corte Suprema quedaron plasmadas en el Acta 151-2010, del 24/10/2010: "La especialización ha sido la respuesta a los requerimientos de mayor profundización en las decisiones jurisdiccionales, debido a lo cual se iniciará el estudio destinado a encauzar el

3.1.3. Infraestructura edilicia

En relación a los aspectos de infraestructura del antedicho tribunal, cabe destacar que pese a que no hubo cambios sustantivos a partir de la reforma al proceso penal, lo cierto es que —en términos generales— las instalaciones son adecuadas para dar sustento al nuevo sistema de oralidad implementado en la etapa recursiva. Todas las salas, si bien con diferente organización, cuentan con espacio suficiente para la presencia del público. En promedio, las salas tienen lugar para unas 14 personas, disponiendo para ello de bancos alargados que generalmente están colocados detrás de los escritorios de los intervinientes, y de frente a los estrados del tribunal.

Respecto al espacio destinado para que las partes aguarden ser convocadas para las audiencias, interesa remarcar que ninguna de ellas cuenta con una antesala lo suficientemente adecuada para contener a todas las partes que tendrán que intervenir en esa sala. Casi todas disponen de sillones colocados en el pasillo, aunque generalmente las partes esperan su momento de pie. En este mismo lugar, en las paredes se han colocado pantallas que indican los números de las causas que se estarán viendo en ese día, junto con la tabla a la cual se corresponden. Todas las salas disponen de este sistema, aunque ciertamente no son consultadas con regularidad por ninguno de los litigantes, puesto que se dirigen directamente al oficial.

En cuanto a la ubicación del Tribunal, la mayoría de las salas se hallan en la planta baja del Palacio de Tribunales, y otras tres en el tercer piso. Lo cierto es que no se advierte una clara señalización de ello, en función de que solo disponen de carteles indicativos en la puerta de ingreso a cada uno de los salones.

trabajo en tribunales colegiados, desarrollado a través de salas especializadas, puesto que es una tendencia que se impone cada vez con mayor fuerza en nuestro país, tanto porque a ello conducen las reformas procedimentales de los últimos años, como por la conveniencia en el perfeccionamiento de los jueces, la agilización en la decisión definitiva de las materias puestas en su conocimiento y la necesaria y pretendida unificación de la jurisprudencia. Se acordó que la Comisión compuesta por los ministros señores Nibaldo Segura, Juan Araya, Héctor Carreño y Carlos Kunsemuller, junto al ministro señor Sergio Muñoz, formule una propuesta al Pleno, en el sentido que las Cortes de Apelaciones a las que la ley asigna un mayor número de miembros (Santiago, Valparaíso, San Miguel y Concepción) desempeñen su labor jurisdiccional en salas especializadas, considerando especialmente la visión de aquellas Cortes. Lo anterior fue acordado contra el voto de una señora ministra, quien estimó que el asunto de que se trata debe ser regulado por el legislador".

3.1.4. Sistema de registro

En punto al sistema de registro adoptado por la Corte, se advierte que todas las salas cuentan con micrófonos: tres para los Ministros, uno para el relator, y dos para cada uno de los intervinientes. Todo lo que se expresa en la audiencia es grabado en una computadora bajo la responsabilidad del funcionario de actas, quien archiva cada uno de los audios en relación a cada una de las vistas.[24]

Se ha observado, en escasas ocasiones, que los intervinientes han solicitado una copia del audio de la audiencia al funcionario de actas al cabo de la vista.

3.1.5. Requisitos para la vista de causas: composición del tribunal

Por otro lado, en cuanto a las disposiciones exigidas para dar inicio a las audiencias, es requisito necesario la presencia de tres miembros en el tribunal (CPPChile, art. 356, que en su parte pertinente dispone: "la audiencia solo se suspenderá si no se alcanzare, con los jueces que conformaren ese día el tribunal, el mínimo de miembros no inhabilitados que debieren intervenir en ella"; y del art. 67 del código orgánico de tribunales, que establece: "(l)as salas no podrán funcionar sin la concurrencia de tres jueces como mínimum"). Es por ello que con antelación al comienzo de las audiencias, las partes pueden presentar sus recusaciones o bien los Ministros sus excusaciones, a fin de dar tiempo prudente para que la conformación de la sala pueda lograrse para ese caso.

(24) Respecto al registro de las causas en sistemas informáticos en las Cortes de Apelaciones, Corte Suprema de Chile, Acta 113-2006, 11/07/2006: "Las actuaciones que corresponda realizar ante las Cortes de Apelaciones y Corte Suprema, en el marco de las reformas procesales en lo penal, familia, laboral y provisional, se registrarán en formato computacional y de audio, en su caso, incorporadas a una carpeta informática individual por recurso que sólo se integrará con el registro, en dicho soporte, de los antecedentes que den cuenta de las actuaciones, presentaciones de las partes y resoluciones adoptadas por el tribunal en el curso del procedimiento y que de acuerdo a la ley corresponda registrar. La carpeta informática individual por recurso será respaldada por la Corporación Administrativa del Poder Judicial, mediante sistema computacional en forma diaria, semanal y mensual, conforme a los procedimientos técnicos aprobados y que apruebe en el futuro esta Corte Suprema" (art. 2). Esto se ve reforzado por lo dispuesto en el Auto Acordada 30/05/2005, decretada por la Corte Suprema, relativo a la tramitación en sistema informático de las causas de la reforma procesal penal. En su art. 12 determina que "el registro de la tramitación de la causa, audiencias y resoluciones sólo se efectuará de manera electrónica, al que se integrará el audio. No existirá registro físico escrito".

3.1.6. Personal de las salas. Funciones

En las salas, además de los Ministros, se desempeñan un oficial, un relator, y un funcionario de actas durante el transcurso de las audiencias. No cumplen funciones allí otras personas distintas a ellas.

El oficial es la persona encargada de disponer todo lo materialmente necesario para la celebración de las audiencias, como así también de llamar a los intervinientes para que ingresen en los salones al momento en que deban comparecer. A su vez, son los responsables de confeccionar las tablas a partir de las cuales se organizará la vista de causas en la jornada diaria, y que se publican en carteleras ubicadas en las cercanías de las puertas de entrada de cada sala.

Por su parte, el relator es quien tiene a su cargo informar a los Ministros —en presencia de las partes— cuál es la decisión judicial que generó la interposición del recurso, en qué fecha se dictó, el tipo de recurso del cual se trata, quién es la parte recurrente, y también de poner en conocimiento de los presentes el aspecto puntual del cual ésta se agravia.[25]

Vale hacer una disquisición respecto al rol de los relatores, el cual no se ha mantenido inalterable a lo largo del tiempo. Lo cierto es que previo a la entrada en vigencia del nuevo sistema acusatorio, los relatores concentraban un poder mayor al actual. La función que tenían asignada consistía en realizar la llamada "relación" de lo que ocurría en la causa, predisponiendo a los Ministros de la Corte, si bien las partes podían estar presentes. En estos casos, probablemente, la injerencia del relator era mayor en la solución final del caso, al ser éste quien evaluaba en primer término el expediente, y recién luego se lo transmitía a los Ministros. A su vez, en el antiguo sistema, podía ocurrir que la "relación" sea secreta, en aquellos casos en los cuales se había decretado el secreto de sumario, con lo cual los relatores les presentaban los casos a los Ministros, previo al inicio de la audiencia, en ausencia de las partes.

(25) A través del Auto Acordado del 30/05/2005, la Corte Suprema determinó las funciones de los relatores en el marco del nuevo proceso penal. Así, estableció en su art. 10 que "los relatores de la Corte tendrán como únicas funciones en la vista de los recursos del nuevo sistema procesal penal, dar cuenta al tribunal en los casos establecidos por las disposiciones vigentes, entre ellas de la admisibilidad de los recursos, y servir de Ministro de fe respecto de la realización de la audiencia, mediante firma digital".

Bajo el nuevo sistema, el rol de los intervinientes en general ha sido el de pasar ellos a ser un relator de parte, pues tienen a su cargo explicarle al tribunal el agravio concreto que postulan, y de qué manera entienden que encuadra en alguna de las causales de procedencia reguladas en el código de procedimientos en materia penal.

En cuanto al rol de los funcionarios de actas, tal como adelantáramos previamente, son los encargados de realizar todas las tareas relacionadas con el registro de audio de las audiencias, y quienes entablan comunicación con las partes en aquellos casos en los cuales éstas requieran de una copia del audio de la audiencia, que generalmente es guardada en un pen drive suministrado por el interesado.

3.2 | Organización administrativa y sustanciación del recurso

En este acápite se pretende dar cuenta, por un lado, de los aspectos vinculados con las funciones administrativas de la Corte de Apelaciones de Santiago, en atención al modo por el cual se distribuyen las tareas no jurisdiccionales del tribunal. Por otra parte, también se atenderán separadamente todas las cuestiones relativas al trámite otorgado a los recursos una vez que ingresan al tribunal.

3.2.1. Cuestión preliminar: Organización administrativa de la Corte en relación al sistema de gestión implementado por los juzgados de garantías y tribunales de juicio

Si bien el código orgánico de tribunales dispone que al presidente de la Corte de Apelaciones le corresponden determinadas funciones administrativas con respecto a la organización de las audiencias,[26] lo cierto es

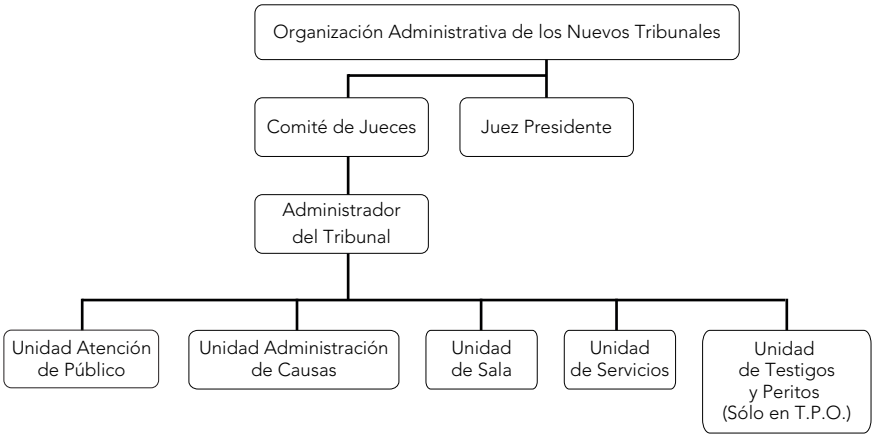
(26) El art. 90 del Código Orgánico de Tribunales establece: "A los Presidentes de las Cortes de Apelaciones, fuera de las atribuciones que otras disposiciones les otorgan, les corresponden especialmente las que en seguida se indican: Inciso 2°: Instalar diariamente la sala o salas, según el caso, para su funcionamiento, haciendo llamar, si fuere necesario, a los funcionarios que deben integrarlas. Se levantará acta de la instalación, autorizada por el secretario, indicándose en ella los nombres de los Ministros asistentes, y de los que no hubieren concurrido, con expresión de la causa que motivare su inasistencia. Una copia de esta acta se fijará en la tabla de la sala correspondiente; Inciso 3°: Formar el último día hábil de cada semana, en conformidad a la ley, las tablas de que deba ocuparse el tribunal o sus salas en la semana siguiente. Se destinará un día, por lo menos, fuera de las horas ordinarias

que las tareas relativas a dar ingreso de los recursos, fijar las fechas de las vistas, y asistir a los Ministros, entre otras, son asumidas derechamente por la Secretaría Criminal del tribunal. Esta oficina se sitúa en la planta baja del edificio de tribunales y no ha sido objeto de cambios sustanciales con motivo del nuevo proceso penal.

A diferencia de este esquema, aunque no se encuentre vinculado estrictamente con el desempeño práctico de la Corte de Santiago, es menester apuntar que los juzgados de garantías y los tribunales de juicio han introducido modernos conceptos de administración a partir del nuevo código, toda vez que se han creado unidades administrativas especializadas, a cargo de un funcionario administrador.

A este respecto, el nuevo diseño puede ser graficado así:[27]

GRÁFICO 1. ORGANIZACIÓN ADMINISTRATIVA DE LOS NUEVOS TRIBUNALES



Como se observa, el nuevo sistema de organización administrativa ha establecido un "comité de jueces" que se debe constituir en todos los juzgados de garantía compuestos por tres o más jueces y en cada uno de los tribunales orales en lo penal, que por definición están integrados por al

de audiencia, para el conocimiento y fallo de los recursos de queja y de las causas que hayan quedado en acuerdo, en el caso del artículo 82."

(27) Véase Carocca Pérez, Alex, *El nuevo sistema procesal penal*, Santiago, Lexis-Nexis, 2005, p. 53.

menos tres jueces. Sus funciones más importantes son las de asumir la superior dirección administrativa y presupuestaria del respectivo tribunal. A su vez, el juez presidente es quien preside el comité, y entre sus funciones le corresponde aprobar los criterios de gestión administrativa y supervisar su ejecución, las que le corresponden al administrador del tribunal.

Respecto a las unidades especializadas, ellas son: Unidad de Sala, encargada de la organización y asistencia a las audiencias; atención de público; Unidad de Servicios, que debe hacerse cargo de la coordinación y abastecimiento físico y material del juzgado y del soporte técnico informático; Unidad de Administración de Causas, que debe llevar el manejo y registro de cada proceso penal, el archivo judicial básico, la actualización diaria de la base de datos y sus estadísticas básicas; y Unidad de Apoyo a Testigos y Peritos —sólo para los tribunales orales en lo penal—, destinada a brindar una rápida atención a los testigos y peritos citados a declarar.

Por otra parte, a partir del nuevo sistema procesal penal, se hizo necesario crear un nuevo funcionario, que debiendo tener un título profesional en las áreas de administración o gestión, asuma la dirección del personal y de la gestión administrativa de los nuevos tribunales. Su denominación es la de administrador de tribunal y se lo define como un auxiliar de la administración de justicia encargado de organizar y controlar la gestión administrativa de los nuevos tribunales. Por eso les corresponde dirigir las labores administrativas del juzgado o tribunal, bajo la supervisión directa del Comité de Jueces del Tribunal.[28]

3.2.2. Presentación de los recursos

Tanto el recurso de apelación como el de nulidad se interponen ante el tribunal que dictó la resolución o sentencia. La regla es que se debe hacer por escrito, con fundamentos de hecho y de derecho, y con peticiones concretas. La excepción está dada para los casos en los cuales el fiscal apela verbalmente la denegatoria de su solicitud de prisión preventiva para el imputado, especialmente cuando el delito endilgado es de aquellos que revisten mayor gravedad. En estos supuestos, la apelación fiscal se satisface solamente con la expresión verbal del representante del Mi-

(28) Carocca Pérez, Alex, *El nuevo..., op. cit.*, pp. 53/56.

nisterio Público en la audiencia preliminar, permaneciendo el imputado privado de su libertad en condición de "detenido en tránsito" hasta tanto ésta decisión sea revisada por la Corte de Apelaciones. Esta excepción a la regla fue consagrada a través de la ley 20.253 de 2008, denominada "Agenda Corta Anti-delincuencia".[29]

3.2.3. Examen de admisibilidad

Una vez presentados, los recursos serán sometidos a una evaluación respecto a su admisibilidad. En el caso del recurso de nulidad, lo harán tanto el tribunal que dictó la sentencia como así también la Corte de Apelaciones que intervenga. En los recursos de apelación, dicho examen estará a cargo solamente del tribunal de base, ya que en la Corte queda a cargo de revisión por la cuenta del relator de la sala respectiva. Este último supuesto permite que al comenzar la audiencia la parte recurrida solicite la inadmisibilidad del recurso, al no haber habido un examen de admisibilidad en el órgano revisor. Estos planteos se han observado en algunas audiencias, debiendo la sala dividir la vista en dos momentos. El primero de ellos dedicado a decidir la admisibilidad del recurso y, en caso afirmativo, dar inicio luego al debate sobre el fondo del asunto traído a resolver.[30]

(29) Con los cambios introducidos por el art. 2, inc. 4, ley 20.253 del 14/03/2008, el inciso segundo del artículo 132 del CPP quedó redactado del siguiente modo: "En la audiencia, el fiscal o el abogado asistente del fiscal actuando expresamente facultado por éste, procederá directamente a formalizar la investigación y a solicitar las medidas cautelares que procedieren, siempre que contare con los antecedentes necesarios y que se encontrare presente el defensor del imputado. En el caso de que no pudiere procederse de la manera indicada, el fiscal o el abogado asistente del fiscal actuando en la forma señalada, podrá solicitar una ampliación del plazo de detención hasta por tres días, con el fin de preparar su presentación. El juez accederá a la ampliación del plazo de detención cuando estimare que los antecedentes justifican esa medida. En todo caso, la declaración de ilegalidad de la detención no impedirá que el fiscal o el abogado asistente del fiscal pueda formalizar la investigación y solicitar las medidas cautelares que sean procedentes, de conformidad con lo dispuesto en el inciso anterior, pero no podrá solicitar la ampliación de la detención. La declaración de ilegalidad de la detención no producirá efecto de cosa juzgada en relación con las solicitudes de exclusión de prueba que se hagan oportunamente, de conformidad con lo previsto en el artículo 276".

(30) Estos casos se encuentran contemplados en el art. 11 del Acta 113-2006 del 11/07/2006, que respecto a la admisibilidad del recurso de apelación sostiene: "En los recursos de apelación, el pronunciamiento de admisibilidad se efectuará con la cuenta del relator por la sala respectiva, previo al conocimiento del fondo, el día fijado para la audiencia, salvo que el tribunal acuerde oír a los abogados de las partes al respecto, caso en el cual se les invitará a exponer sus alegaciones sobre el particular en la misma audiencia".

3.2.4. Elevación de antecedentes. Ingreso de causas. Asignación de RIT

Superado el examen de admisibilidad, el tribunal de base eleva los antecedentes a la Corte de Apelaciones correspondiente, a través de un sistema informático. La información que se carga en ese sistema, a la que eventualmente tienen acceso los Ministros de la Corte, es la transcripción de la resolución recurrida; las pistas de audio de las audiencias; y el escrito del recurso interpuesto.(31)

El ingreso de causas en la Corte se efectúa a través de la Secretaría Criminal, mediante interconexión electrónica con los diversos tribunales haciendo uso del sistema informático.(32) De allí se extraen, en versión digital, los escritos necesarios para identificar la complejidad del recurso, de manera que con esa información se puedan programar las vistas de las causas.

Al ingresar el recurso en la Secretaría, se le asigna en la Corte un Rol Interno del Tribunal (RIT), que se lleva anualmente y de manera correlativa sin perjuicio de mantener visible el Rol Único de Causa (RUC), conforme a la tipología general dispuesta por la Corte.(33)

3.2.5. Confección de las tablas de causas

Elevados los antecedentes a la Corte de Apelaciones, y una vez ingresado el recurso en la Secretaría Criminal, la causa se coloca "en tablas". Al no haber salas especializadas, lo cierto es que coexisten distintas tablas con diferentes órdenes de preferencia en relación al área respectiva. La principal distinción está dada por las tablas ordinarias y la extraordinaria. Ésta

(31) En cuanto a la remisión de los antecedentes al tribunal *ad quem*, Acta 113-2006 del 11/07/2006: "Concedido un recurso por el tribunal a quo u ordenado remitir los antecedentes para su conocimiento y resolución por el tribunal ad quem, se enviará u obtendrá copia del registro computacional y de audio, además de trascripción íntegra de la resolución impugnada, copia electrónica de la presentación por la cual se interpone el recurso, de la resolución que lo concede, de la individualización del Juez, de las partes o de los intervinientes, de los apoderados de éstos, y de la forma señalada para su notificación. Si por cualquier motivo estuviere suspendido el funcionamiento del Sistema Informático, el tribunal respectivo deberá remitir copia de la carpeta electrónica de la causa, esto es, el registro informático en soporte material que contendrá los antecedentes antes referidos consignados en un procesador de texto Word. El ingreso de los recursos que se interpongan directamente ante las Cortes de Apelaciones, seguirá las reglas generales y las relativas a la presentación de escritos" (art. 4).

(32) De conformidad con lo establecido en el art. 3 del Acta 113-2006.

(33) De conformidad con lo establecido en el art. 5 del Acta 113-2006.

última es aquélla que siempre guarda preferencia respecto al resto, pues consiste en todas las apelaciones de causas de la reforma procesal penal vinculadas con cuestiones de libertad. Con lo cual, la vista de causas en cada Sala estará encabezada diariamente por éstos últimos recursos.

En este sentido, el cuadro de preferencia de las tablas es el siguiente:

1. Extraordinaria Penal (Libertades-Reforma Procesal Penal).
2. Agregadas (Amparos, excarcelaciones del sistema antiguo, recursos de protección, y otras leyes especiales).
3. Radicadas
4. Ordinaria Reforma
5. Ordinaria
6. Minutas de Cuenta

En relación a la elaboración de estos listados, el Acta 113-2006 de la Corte Suprema de Chile establece que "se confeccionará diariamente, por Sala, la tabla de causas agregadas extraordinariamente en que se designará la audiencia en que habrá de ser vista", agregando que "siguiendo igual proceder, el día viernes de cada semana se confeccionará la tabla ordinaria, la que será sorteada entre las distintas Salas, en su caso. La formación y confección de estas tablas quedará bajo la supervisión del señor Presidente y de la Secretaria de la Corte".

Esto es, que las causas extraordinarias se incluyen regularmente en primer lugar en la vista de cada Sala, mientras que las ordinarias se publican los días viernes por la tarde para la semana siguiente.

3.2.6. Comparecencia de las partes

Una vez que la causa se encuentra colocada "en tablas", los abogados que las litigarán deben ir el día en que los hayan asignado y, entre las 8 y 8.30 am, se deben anotar en un listado que se halla en la mesa de la sala que corresponda.[34] Esto significa que efectivamente han comparecido y que quieren alegar, permitiéndole al oficial de sala llevar un registro de

(34) "Los abogados que quisieren hacer uso de su derecho a alegar deberán anunciarse personalmente con el respectivo Relator antes del inicio de la audiencia en la que deba verse la causa indicando el tiempo aproximado que emplearán en su alegato circunstancia que se hará constar en el expediente"(art. 5, Auto Acordada, 02/09/1994).

cuáles son las causas que cuentan con la presencia de los intervinientes para la vista respectiva.

Diariamente, las tablas son colocadas en un mostrador ubicado en la entrada de cada una de las salas, en el cual los abogados litigantes identifican en qué orden ha quedado la causa en la cual deben alegar.

Tras ello, las partes deben aguardar a ser llamadas en la antesala, pues —como se ha dicho en el apartado anterior— el orden de vista depende de la preferencia asignada para cada tabla.

En esta línea, puede suceder —de hecho, acontece a menudo— que un litigante esté alegando en una sala y sea llamado para comparecer en otra. En estos casos, la subsanación depende del criterio de cada sala. En algunas de ellas se ha establecido dejar esa causa para el final del día, y en otras —la mayoría— se avanza con la causa siguiente hasta que el abogado litigante regrese de la otra sala.

A partir de los inconvenientes surgidos por la superposición de audiencias, algunos litigantes optan por dejar asentado en el listado de causas diarias que también estarán alegando en otra sala, indicando en cuál de ellas estará, de manera que incluso el oficial pueda acercarse hasta allí para verificar que en ese momento el abogado está litigando otro recurso.

3.3 | Dinámica de la audiencia

Este apartado estará dedicado al abordaje del modo en que se desarrollan las vistas de causas ante la Corte de Apelaciones de Santiago, puntualizando fundamentalmente en la forma a través de la cual los comparecientes presentan y litigan sus agravios, el grado de intervención en la audiencia de los Ministros que conforman el tribunal y, finalmente, la manera por la cual se adoptan las decisiones judiciales.

3.3.1. Presencia de público

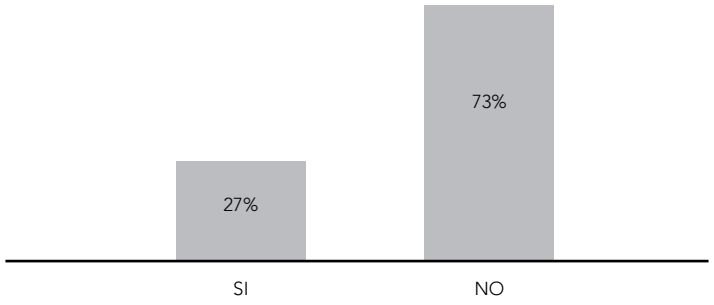
Si bien las audiencias celebradas en la Corte de Apelaciones son públicas, lo cierto es que para ingresar a las salas se le debe avisar al oficial que corresponda. Frente a esta petición, dependiendo del criterio de cada sala, puede suceder que la autorización para el ingreso esté sujeta a la

conformidad de los Ministros que integran el Tribunal, o bien incluso de los propios litigantes que se encuentran allí aguardando a ser llamados. También puede ocurrir que no se presente ningún tipo de reparo, aunque igualmente ha acontecido que al público se le formulen preguntas al estilo de por qué se quiere ingresar, con qué fin, de cuál institución viene, si es familiar de un imputado, etcétera.

De manera positiva, en la generalidad de los casos no se han exteriorizado mayores objeciones para presenciar las vistas en la Corte.

En cuanto a la asistencia de público, del total de las audiencias presenciadas, se ha concluido que en un porcentaje del 73% no hubo personas en la sala. En cambio, en un 27% de las mismas sí hubo, generalmente familiares de los imputados, y particularmente en relación a casos que se vinculaban con la imposición de medidas de coerción personal restrictivas de la libertad ambulatoria.

GRÁFICO 2. PRESENCIA DE PÚBLICO EN LAS AUDIENCIAS



Fuente: Elaboración propia sobre la base de la observación de 29 audiencias.

Respecto a este tema, es menester resaltar lo dicho en punto a la falta de señalización sobre la ubicación de las salas de audiencias de la Corte de Apelaciones, las cuales solamente cuentan con un cartel indicativo de la sala de la cual se trata, colocado en la parte superior de la puerta de ingreso.

Este aspecto coadyuva a la ausencia de público externo que presencie y, en definitiva, también ejerza un control fehaciente de la actividad jurisdiccional que tiene lugar en éste tipo de audiencias de revisión.

3.3.2. Iniciación de la audiencia

La vista de la causa comienza generalmente con la solicitud que realiza el Presidente del Tribunal para que las partes intervinientes se identifiquen. Tras ello, le cede la palabra al relator, quien informa de qué causa se trata, de cuál tribunal proviene, quién es el recurrente, cuál es la decisión impugnada, de qué fecha es, y cuál es el pedido concreto que realiza el impugnante. Acto seguido, el presidente de la sala puede o no solicitar mayor información al relator acerca del caso. De las audiencias observadas, se desprende que en muy pocas ocasiones ello ha sucedido, pues en la generalidad de las vistas, tras la presentación del caso, se le da la palabra directamente al recurrente con el fin que ejerza su derecho al alegato, tal como se lo expresa.

En la mayoría de los casos, el presidente del Tribunal le indica a quien exponga en primer término el tiempo con el que cuenta para presentar sus agravios, que en casi todas las oportunidades se aproximó a los diez o quince minutos. En otros casos, los tiempos se extendieron a los treinta o cuarenta minutos, dependiendo de la complejidad de la discusión. Incluso, en otros supuestos, la propia parte informa oralmente al Tribunal el plazo temporal que le insumirá su exposición.

Sin perjuicio de ello, tal como hemos apuntado previamente, suele suceder que los litigantes —al presentarse en la sala que tendrán que intervenir— dejan asentado en el listado de causas el tiempo que les insumirán sus exposiciones. Aunque lo cierto es que generalmente ese tiempo luego es establecido o conversado con el presidente del Tribunal.

3.3.3. Exposición de agravios

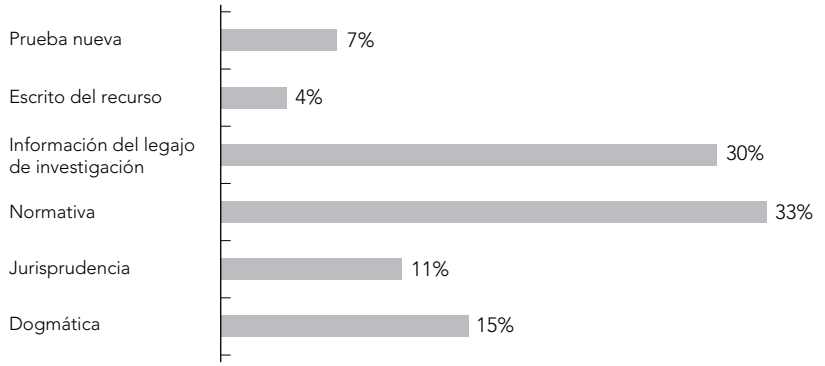
Una vez que los Ministros escucharon la información proveída por el/la relator/a, y el presidente del Tribunal indicó los tiempos de exposición, la parte recurrente es siempre la primera en tomar la palabra.

Al dar inicio a la presentación de la impugnación, ésta última parte generalmente menciona los artículos en los cuales asienta su pretensión. Luego, realiza una introducción respecto a los antecedentes del caso, remitiendo habitualmente a la carpeta investigativa del fiscal, en aquellas vistas que se trataran de recursos de apelación contra resoluciones del juez de garantías.

Sobre el particular, es necesario destacar que los antecedentes del caso son siempre introducidos por la parte recurrente, ocurriendo en algunas oportunidades que los propios Ministros profundizan en ellos haciendo preguntas concretas.

En función de las audiencias observadas, a continuación veremos el contenido con el cual los recurrentes han dotado a la presentación de sus agravios en los supuestos del recurso de apelación:

GRÁFICO 3. CONTENIDO DE LOS AGRAVIOS EN RECURSOS DE APELACIÓN



Fuente: Elaboración propia sobre la base de la observación de 29 audiencias.

A partir de este gráfico, se advierte que en una gran cantidad de casos, los impugnantes basaron la presentación de sus agravios en el incumplimiento de la normativa vigente (33%), como así también en las constancias que obran en la carpeta de investigaciones del Ministerio Público (30%).

En menor medida, se observa que los litigantes también hicieron uso de fragmentos dogmáticos (15%), o de antecedentes jurisprudenciales (11%) sobre el tema materia del recurso.

En ocasiones puntuales, los recurrentes han dotado de contenido a la exposición de sus agravios en función de los fundamentos o testimonios que habían esgrimido en el escrito de interposición del recurso, como así también ha ocurrido que el litigante produjo prueba nueva (generalmente, vinculada con las condiciones personales del imputado al momento de solicitar que se deje sin efecto la prisión preventiva).

3.3.4. Intervención de la parte recurrida

Una vez que el recurrente planteó sus agravios, y exhortó al tribunal en virtud de su solicitud, el presidente de la sala le concede la palabra a la parte recurrida a fin de que exponga los motivos por los cuales entiende que no se debe hacer lugar el recurso.

En la mayoría de los casos observados, se advierte que la parte no recurrente alegó sus argumentos aisladamente, sin conexión con los planteamientos efectuados por la contraparte. Ello se debe, entendemos, en gran medida a la escasa práctica en destrezas de litigación en el marco de audiencias orales en la etapa recursiva. Los argumentos se presentan de modo aislado, principalmente porque no se atienden con precisión cuáles son los puntos de la contraparte que deben ser contrarrestados en una audiencia de éstas características.

En esta dirección, vale señalar que la actividad recursiva estructurada oralmente requiere por parte de los litigantes que ellos mismos introduzcan los antecedentes, y presenten sus agravios remitiendo puntualmente al motivo que lo generó en virtud de la audiencia anterior. Es decir, se les exige un análisis de rigor de la causa, de modo tal que la audiencia del recurso esté focalizada en la demostración de que efectivamente se causó un perjuicio, y que éste debe ser subsanado mediante la modificación de la resolución de grado.

Además, en sentido positivo cabe resaltar que en todas las vistas analizadas se produjo una réplica y contra réplica entre las partes, favoreciendo la contradicción entre los planteos esgrimidos. Esto se perfeccionó en exiguas ocasiones, pues se vincula estrechamente con el rol proactivo de conducción del Ministro Presidente del Tribunal, que en la generalidad de las vistas se relacionó con una pasividad en la promoción del debate.

3.3.5. Rol de los Ministros de la Corte

En éste acápite se analizará uno de los aspectos más relevantes respecto del funcionamiento de la Corte de Apelaciones de Santiago. Aquí abordaremos la actividad de los Ministros durante el transcurso de la audiencia, principalmente en relación a su rol a la hora de adquirir información sobre los casos, como así también el grado de intervención en pos de instalar prácticas que guarden vinculación con la lógica de la oralidad en la etapa recursiva. En

términos generales, se pretende observar cuál es la concepción subyacente que los magistrados tienen en punto al nuevo sistema de recursos.

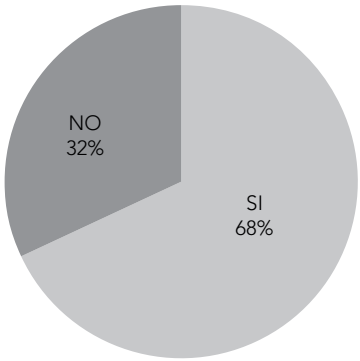
En primer término, interesa apuntar que —de las audiencias observadas— se advierte un cierto grado de pasividad por parte de los Ministros, en cuanto es escasa su intervención en el desarrollo del debate. Ello debido a que solo se limitan a conceder la palabra a los intervinientes, lo cual produce que las vistas se transformen en alegaciones aisladas, que en muy pocos casos se concentran en el punto objeto del recurso. En ocasiones puntuales, se ha observado que el Ministro conductor de la audiencia indicó a los intervinientes que se centralicen en discutir el agravio introducido por el recurrente, evitando permanentemente que las alegaciones sean abstractas y no conduzcan al punto en concreto, e incluso realizando preguntas sobre lo expresado por las partes. De las diez salas de la Corte, ésta conducta se ha evidenciado con claridad en tan solo una de ellas, lo cual —en términos generales— permite inferir que existe una reacia actitud por parte del tribunal hacia la concepción de la audiencia como instrumento de trabajo para la producción de sentencias, compatible con un sistema oral de adopción de decisiones judiciales en la fase recursiva.

3.3.5.1. Formulación de preguntas

Ahora bien, del total de las audiencias observadas, la mayoría de los Ministros formularon preguntas a las partes. Ello no obsta puntualizar que en realidad esas intrusiones se realizaron habitualmente al cabo de los alegatos, una vez que las abstracciones de los planteos habían quedado configuradas. Es decir, una vez que los agravios ya fueron introducidos, sin posibilidad de que se le exija a la contra parte —y, también, a la recurrente— que demuestren cuál era la afectación puntual que ameritaba la modificación de la resolución, o bien por qué precisamente se debía descartar ese planteo en base a elementos concretos de la causa. En este punto, es central el rol que adquiera el juez para evitar la dispersión de los argumentos de las partes, pues su adecuada intervención permitirá generar decisiones que se sustenten sobre información de alta calidad que haya surgido del intercambio entre los intervinientes.

En este marco, a continuación veremos gráficamente un porcentual de los casos en los cuales los Ministros de la Corte formularon preguntas a las partes:

GRÁFICO 4. ¿LOS JUECES FORMULARON PREGUNTAS A LAS PARTES?



Fuente: Elaboración propia sobre la base de la observación de 29 audiencias.

De lo mostrado se desprende que, en un 68% de las audiencias observadas, los Ministros efectivamente efectuaron realizaron preguntas a fin de indagar acerca de alguna cuestión puntual del alegato. Sin embargo, tal como hemos dicho, en su mayoría, las preguntas de los Ministros no se vincularon con la necesidad de delimitar el debate al punto de agravio, sino que se efectuaron al final de la audiencia, y en relación con cuestiones que no habían sido lo suficientemente claras durante las exposiciones y que luego eran corroboradas con los antecedentes informáticos de la causa.

Esto equivale a decir que, si bien se realizan preguntas, ellas no están dirigidas a delimitar el ámbito de discusión en el marco de la audiencia, sino que continúan siendo compatibles con un formato rígido y formal en donde las alegaciones se realizan apartadamente, sin que los jueces pretendan generar un real contradictorio entre ellas.

Este aspecto guarda estricta relación con la diferencia entre las audiencias de la etapa preparatoria y la audiencia de juicio oral, puntualmente en atención al rol que le cabe al juez. Al respecto, se ha dicho que

> "en tanto en un juicio se pretende que el tribunal o juez de sentencia se mantengan lo más distantes posibles de la producción de información, permitiendo que las partes produzcan su prueba en la forma en que lo estimen conveniente, en una audiencia de la etapa preparatoria no sólo es posible sino que

> en algunos casos resulta enormemente necesario que el juez asuma un rol activo en la aclaración de ciertos puntos".[35]

Sobre éste último punto, cabe señalar que la generalidad de las audiencias observadas en la Corte de Apelaciones eran revisiones de decisiones adoptadas durante la investigación penal preparatoria, lo cual significa que la actitud del juez del recurso se debe corresponder con la misma que le cabe al juez de garantías.

Desde esta perspectiva, es posible afirmar que resulta imprescindible que el juez, como conductor de la audiencia en el tribunal del recurso, intervenga realizando preguntas aclaratorias, consultando sobre el respaldo de información que las partes tienen, impidiendo que las discusiones se desvíen del (o los) objetivo que motivó la audiencia.[36]

3.3.5.2. Consulta a los escritos de la causa

Por otro lado, a su vez, se observa que en algunos casos los Ministros acudieron a los escritos de apelación o los antecedentes informáticos de la causa, tanto para tener información previa al comienzo de la audiencia, como así también a posteriori para corroborar que la presentación de los intervinientes se condiga realmente con lo sucedido en la audiencia que motivó el recurso.

Ésta práctica remite en realidad al antiguo sistema en el cual el expediente dominaba el acceso a la información de la causa que los jueces debían leer para resolver. A partir de la consagración de un esquema procesal por audiencias, las actas escritas se reducen meramente a la indicación del tema del cual se trata el remedio judicial, realzándose la importancia de la audiencia oral como escenario de presentación de los antecedentes del caso, de alegación de los fundamentos del recurso, y del contradictorio necesario con la contraparte. Esto es, la centralidad de la audiencia como

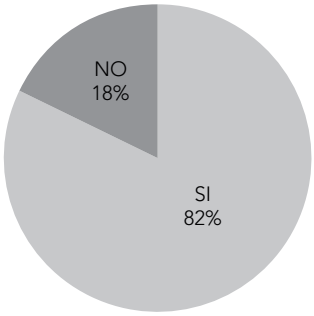
(35) Lorenzo, Leticia; Lima Magne, Juan José; Maclean Soruco, Enrique y Lima Magne, Iván, *Manual de Litigación en Audiencias de Medidas Cautelares, Asociación Internacional de Juristas*, La Paz, CEJIP, 2009, p. 37.

(36) *Ibíd.*, p. 38. El punto central en el que radica la diferencia entre los roles del juez de juicio y de garantías consiste en que el primero de ellos se limita a observar la producción de prueba que realizan las partes, mientras que el otro —durante las audiencias previas al juicio— debe tener una actitud proactiva en busca de la información que los intervinientes alegan, y que no puede ver toda vez que la evidencia está contenida en los legajos de cada una de las partes.

espacio de toma de decisiones judiciales relevantes, y como metodología de acceso a la información.

En el siguiente cuadro veremos en qué porcentual de las audiencias los Ministros acudieron a los antecedentes escritos o informáticos de la causa, con la intención de ser ellos mismos la fuente de aprovisionamiento respecto a las referencias sobre el caso.

GRÁFICO 5. ¿CONSULTAN LOS JUECES ALGÚN ESCRITO?



Fuente: Elaboración propia sobre la base de la observación de 29 audiencias.

3.3.5.3. Concepción que tienen los Ministros sobre el sistema recursivo actual

En suma, se coligen dos conclusiones preliminares respecto al rol de los Ministros y la lógica de trabajo que emplean en esta etapa procesal.

Por un lado, se advierte que si bien la mayoría de los magistrados intervienen efectuando preguntas a las partes con el fin de desasnar los antecedentes o fundamentos, lo cierto es que tales indagaciones no guardan vinculación certera con el necesario contradictorio que se debe generar a fin de que sean las partes las que puntualmente debatan en concreto los agravios que dieron motivo a la interposición del recurso. Caso contrario, ocurre lo que finalmente sucede en la Corte de Apelaciones: alegaciones genéricas y abstractas, alejadas de las circunstancias particulares del caso. Ello se observa con claridad absoluta en las discusiones relacionadas con los requisitos exigidos para la aplicación del encarcelamiento preventivo. De las audiencias de revisión de esta medida, se observa que en escasos casos los debates se vincularon a la acreditación de los riesgos procesales en el caso particular de los encartados, pues en realidad las alegaciones giran en torno al monto de pena en expectativa, la peligrosidad del delito endilgado o incluso los supuestos legales previstos en el código. Esto claramente es perfectible a

partir de la participación activa del Ministro que conduce la audiencia, quien tendría que guiar el debate hacia el punto que dilucidará la cuestión. En estos casos, una adecuada conducción propiciaría indagar puntualmente acerca de las circunstancias personales del imputado, aclarando que no se tendrán en cuenta argumentos que excedan esos parámetros. Permitir alegaciones individuales contribuye en definitiva a alimentar los vicios del sistema escrito en el cual cada parte "dictamina" sin ahondar en los agravios concretos.

Por otra parte, se desprende que los Ministros de la Corte, en su mayoría, continúan trabajando bajo la lógica del "expediente" como fuente de información. Ello debido a que en muchas ocasiones requieren necesariamente tomar contacto con los antecedentes del caso para resolver en la audiencia. Puede ocurrir que tomen conocimiento de ellos con antelación al comienzo de la vista, o incluso tras su finalización, siendo los relatores quienes suministran esos datos a pedido de los magistrados.

Esto se ve reforzado en atención a lo conversado en ciertas entrevistas entabladas con algunos Ministros de la Corte, quienes refirieron que "se sienten más cómodos trabajando con el papel", o incluso que "no se está suficientemente informado sobre el problema", haciendo alusión a la posible falta de autosuficiencia de los alegatos que formulan las partes en el transcurso de la audiencia.

En efecto, las justificaciones expuestas por los Ministros demuestran que subrepticiamente continúan latentes los vestigios de una cultura escrita, que desconfían de las intervenciones de los litigantes, y que en realidad deben ser ellos mismos quienes subsanen la "falta de preparación" de las partes acudiendo a los escritos, a las transcripciones de las resoluciones, y a las pistas de audio de las audiencias que motivaron la interposición del recurso, todo lo cual no hace más que robustecer la idea de que la audiencia del recurso se transforma en un espacio formal en el cual los intervinientes formulan sus peticiones genérica y abstractamente, y los Ministros no puntualizan en el agravio concreto, porque en definitiva serán ellos mismos quienes sean los encargados de chequear la fiabilidad de los argumentos, y confrontarlos con lo sucedido en la audiencia.

3.3.6. Deliberación. Resolución

En esta sección se propicia dar cuenta del modo por el cual los Ministros de Corte adoptan sus decisiones, tanto en relación a la construcción de la

resolución tras la audiencia, como así también respecto al contenido del cual las dotan.

De las audiencias observadas se advierte que una vez superadas las réplicas y duplicas entre las partes, el presidente de la sala decreta la suspensión de la vista. También se ve que en todos los casos, los Ministros se quedan en el mismo sitio a fin de deliberar.

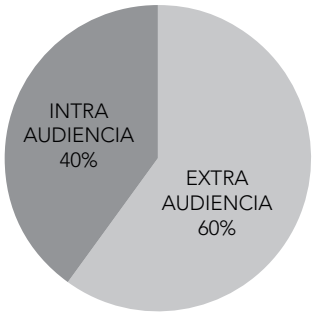
Dependiendo del criterio de cada sala, los intervinientes permanecen allí presentes, o bien son invitados a aguardar en la antesala, mientras los magistrados reflexionan respecto a la solución que tomarán.

No se advierte una preeminencia de alguno de estos dos formatos, pues en realidad, de las audiencias observadas, se colige que ambos se presentan en igual cantidad de oportunidades.

El momento de la adopción de la decisión se sujeta al tipo de recurso que tendrán que resolver los magistrados. Los de apelación son decididos inmediatamente al cabo de la audiencia, más aún si el objeto se vincula con una medida de coerción personal. En el caso de los recursos de nulidad, si bien en ciertos casos son resueltos luego de la audiencia, la generalidad es que la causa quede "en acuerdo", en cuyo caso los Ministros cuentan con 20 días para decidir y redactar la sentencia.

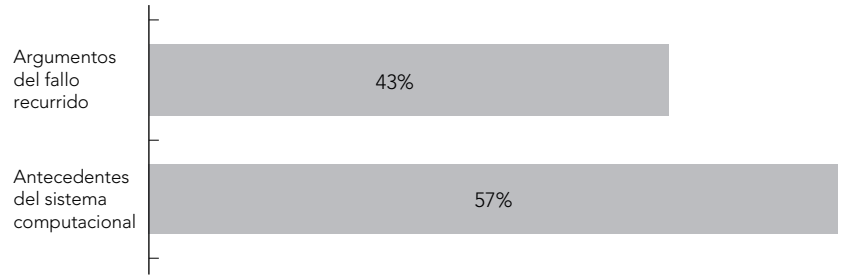
Interesa ahondar en cuáles son los argumentos escogidos por los Ministros a la hora de fundar la decisión que adoptaron, puntualizando si la información utilizada se generó en el entorno de la audiencia, o bien si se usaron antecedentes que reunidos por fuera de ella:

GRÁFICO 6. LUEGO DE DELIBERAR,
¿CON QUÉ INFORMACIÓN SE FUNDA LA DECISIÓN?



Fuente: Elaboración propia sobre la base de la observación de 29 audiencias.

GRÁFICO 7. ¿CUÁL ES LA INFORMACIÓN EXTRA AUDIENCIA UTILIZADA?



Fuente: Elaboración propia sobre la base de la observación de 29 audiencias.

En el lapso de tiempo con el que se cuenta al quedar la causa "en acuerdo", los magistrados pueden consultar los antecedentes del caso que están en el sistema informático. En algunas oportunidades, de lo conversado con algunos de ellos, se desprende que también escuchan los audios de la audiencia celebrada en la Corte de Apelaciones, con la intención de controlar la veracidad de los agravios en función de su confrontación con la audiencia que motivó el recurso. Esto último es justificado bajo el argumento de que "la decisión no saldría bien fundamentada" porque aducen que "los intervinientes no están bien preparados". Otros Ministros, por el contrario, sostienen que las audiencias son autosuficientes para resolver, porque en realidad son los propios interesados quienes deben introducir los antecedentes, y los Ministros deben preguntarles a ellos toda la información que requieran para resolver.

En suma, entendemos que la mejor solución es el formato adoptado por los Ministros que conciben de éste último modo al sistema oral de recursos, pues ciertamente la audiencia se debe consolidar como una metodología de trabajo en la cual las decisiones judiciales sean su resultado final, y en la cual las partes puedan ejercer razonablemente sus derechos.

3.4 | Información estadística sobre los tiempos procesales en la Corte de Santiago

En esta sección haremos un análisis de los datos estadísticos vinculados a la tasa de demora en la sustanciación de los recursos en la Corte de Apelaciones de Santiago. Ahora bien, a estos fines, cabe puntualizar que se utilizará solamente la información proveída por la Defensoría Regional

Norte, la cual tiene a su cargo más del 50% de las causas que tramitan ante la Corte, atento a que ha resultado difícil contar con los datos sobre el total de los recursos.

Las estadísticas que se presentarán operan en diferentes niveles, toda vez que se hará una disquisición entre los tiempos de demora propios de la gestión administrativa y de la función jurisdiccional, y por último, del funcionamiento general del tribunal, tanto en lo concerniente a los recursos de apelación como de nulidad.

Toda esta información puede ser graficada de la siguiente manera:

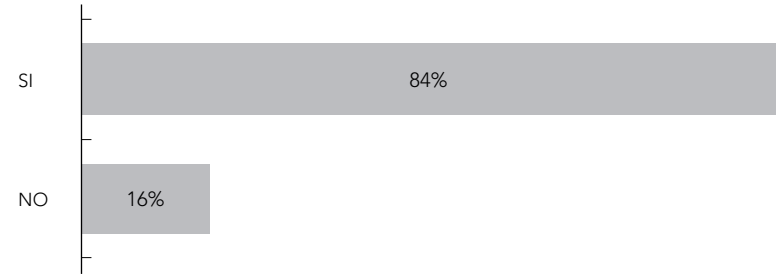
TABLA 1. ESTADÍSTICAS DEL PRIMER SEMESTRE (ENERO-JUNIO) DEL AÑO 2013

Gestión administrativa	
Tasa de demora promedio entre ingreso del recurso (apelación/nulidad) a la Corte y fecha de la vista de la causa	19,80 días
Función jurisdiccional	
Tasa de demora promedio entre la vista de la causa (apelación/nulidad) y fecha de lectura de la resolución	2,33 días
Funcionamiento general del tribunal	
Tasa de demora promedio entre ingreso del recurso (apelación/nulidad) a la Corte y fecha de lectura de la resolución	21,91 días

Fuente: Elaboración propia sobre la base de las estadísticas proveídas por la Base de Datos de la Unidad de Estudios, Defensoría Regional Metropolitana Norte.

A continuación, veremos en qué porcentaje estos casos se han decidido en audiencias:

GRÁFICO 8. ¿SE RESOLVIÓ EN AUDIENCIA?



Fuente: Elaboración propia sobre la base de las estadísticas proveídas por la Base de Datos de la Unidad de Estudios, Defensoría Regional Metropolitana Norte.

Pues bien, hasta aquí hemos visto que, en lo que respecta a la función administrativa consistente en practicar el ingreso de las causas y fijar su vista en la Corte, transcurren un promedio de 19,80 días, tomando como base los recursos resueltos durante el primer semestre del año 2013. A su vez, se ha observado que, en relación a la función jurisdiccional relativa a la resolución de los casos tras la audiencia, el tiempo promedio es de 2,33 días, de lo cual es posible concluir que casi la totalidad de los recursos son resueltos en el marco de la vista. Con esta afirmación es consistente la gráfico 8, en tanto allí se advierte que el 84% de los casos son decididos como producto de un trabajo realizado en audiencia. Por último, en términos generales, se pudo ver que la duración promedio del trámite del recurso —entre que ingresa a la Corte y se resuelve— es de aproximadamente 21,91 días.

Por otra parte, en lo que sigue veremos con precisión los tiempos en que se resuelven los recursos de apelación, por un lado, y de nulidad, por el otro, de modo que pueda ponerse de resalto de qué modo tramitan cada uno de ellos:

TABLA 2. DISQUISICIÓN ENTRE TIEMPOS DEL RECURSO DE APELACIÓN Y NULIDAD

Recursos de apelación	
Tasa de demora promedio entre ingreso del recurso a la Corte y lectura de la resolución	11,92 días
Recursos de nulidad	
Tasa de demora promedio entre ingreso del recurso a la Corte y lectura de la resolución	51,57 días

Fuente: Elaboración propia sobre la base de las estadísticas proveídas por la Base de Datos de la Unidad de Estudios, Defensoría Regional Metropolitana Norte.

De lo expuesto, se observa que los recursos de apelación —que pueden ser presentados con motivo de una medida cautelar, sobreseimientos definitivos o temporales, la revocación de beneficios, exclusiones de prueba, suspensiones condicionales del procedimiento, montos de costas, entre otros— demoran un promedio de 11,92 días entre el ingreso al tribunal y su resolución. Mientras que, los recursos de nulidad —generalmente procedentes en contra de sentencias definitivas— tienen una tasa de promedio de 51,57 días desde que se practica su ingreso por la Secretaría Criminal hasta que se resuelve.

4 | Consideraciones finales

4.1 | Los beneficios de la oralidad en la actividad recursiva

La experiencia chilena en relación a la oralización de la fase impugnativa nos permite extraer dos conclusiones generales: por un lado, que es posible diseñar un régimen de recursos consistente con los parámetros de un paradigma acusatorio —entre ellos, la centralidad política del juicio en el proceso—, y, por otra parte, que la oralidad es el instrumento más contundente para abrir brechas en la cerrada tradición inquisitiva.

Sobre este último aspecto, son incuestionables las ventajas que posee el diseño de un sistema oral para la fase recursiva por sobre uno escrito, máxime si ésta comparación se efectúa en base a las exigencias que impone la garantía fundamental del juicio previo.

Desde esta perspectiva, un sistema de impugnaciones sustentado en la lectura de un registro de actas, o del expediente, produce un conjunto de afectaciones severas a la garantía en cuestión. Al respecto, se podrían identificar tres motivos bien definidos: en primera instancia, la figura del expediente trae como consecuencia la desaparición de la inmediación, en tanto el juez sólo toma conocimiento de la causa a partir de su lectura, no tiene contacto personal con las partes ni conoce al imputado. Más, desde que lee todas las actuaciones hasta que dicta la sentencia, existe una ruptura de continuidad, de modo que el juez se ocupa de otros asuntos, sigue firmando su despacho, atendiendo cuestiones administrativas, etcétera. En segundo lugar, otra forma de violar el juicio previo tiene relación con la "delegación de funciones", puesto que en muchos tribunales de nuestros países no son los jueces quienes verdaderamente dictan las sentencias, sino que en realidad las decisiones son tomadas por un subalterno. Por último, en tercera instancia, una afectación sistemática al principio del juicio previo se vincula con la falta de deliberación. En tribunales colegiados, la práctica forense ha desnaturalizado la idea del debate, de la mano de la sobrecarga de trabajo, con lo cual se ha cambiado la deliberación, que es eminentemente un proceso de construcción conjunta, por la aprobación escrita de proyectos de sentencias.[37]

(37) Binder, Alberto, *Introducción..., op. cit.*, pp. 111 y ss.

De este modo, estamos en condiciones de afirmar que el juicio previo opera como una limitante política al poder penal del Estado, toda vez que exige un proceso judicial penal que sea diseñado bajo una serie de formas específicas.

Una de ellas consiste, indudablemente, en la necesaria oralización del trámite recursivo, lo cual redunda en la construcción de un régimen de control de las decisiones judiciales compatible con la garantía objeto de análisis. Es por ello que Binder afirma que

> "cuando hablamos de 'oralidad' no estamos diciendo simplemente las actuaciones de roles escénicos en un espacio más o menos majestuoso. De lo que se trata es de lograr pasar de un modelo de administración de justicia basada en el trámite, en la petición (que es el modelo de las peticiones administrativas) a una administración de justicia basada en el litigio. La estructura del litigio es un punto fundamental como eje articulador de las distintas propuestas de cambio. De allí que no sea extraño que la tradición inquisitorial —una tradición de justicia sin litigio— se ensañe con el juicio y las audiencias orales".(38)

En virtud de todas estas razones, consideramos necesario emprender una transformación sustancial en relación al modo por el cual se revisan las resoluciones judiciales en un proceso penal. Este cambio debe estar vinculado a una noción moderna que conciba al sistema de audiencias orales como una metodología de trabajo para la toma de decisiones, reuniendo a los actores involucrados en la decisión, y coadyuvando —al mismo tiempo— a la efectiva consolidación de los principios de publicidad, contradicción e inmediación en la actividad recursiva.

(38) Binder, Alberto, "La fuerza de la oralidad", en *La implementación de la nueva justicia penal adversarial*, Bs. As., Ad-Hoc, 2012, p. 180.

Fuentes citadas

Índice de fuentes citadas

AAVV, "Reformas Procesales Penales en América Latina", en *Revista Sistemas Judiciales*, nº 3, 19/08/2002.

Aboso, Gustavo E. y Zapata, María F., *Cibercriminalidad y derecho penal*, Bs. As.-Montevideo, B de F, 2006.

Aboso, Gustavo, *Código Penal de la República Argentina comentado, concordado y con jurisprudencia*, B de F, Buenos Aires-Montevideo, 2012, pp. 575 y ss.

Amans, Carla V. y Nager, Horacio, *Manual de Derecho Penal. Parte Especial*, Bs. As., Ad-Hoc, 2009.

Amelotti Nicolás y Bahamondes Santiago, "La audiencias orales ante la Cámara del Crimen de la Capital Federal. Un análisis práctico de la reforma introducida por la ley 26.374", *en Revita jurídica La Ley*, 2009-F-1202.

Anarte Borrallo, Enrique, "Incidencia de las nuevas tecnologías en el sistema penal. Aproximación al derecho penal en la sociedad de la información", [en línea] http://www.uhu.es/derechoyconocimiento/DyC01/A12.pdf

Arocena, Gustavo, "De los delitos informáticos", en *Revista de la Facultad de Derecho, Universidad Nacional de Córdoba*, vol. 5, nº 1, 1997.

Arruvito, Pedro A., "Ley 26.388. Violación del e-mail o comunicación electrónica", *Doctrina Judicial*, Bs. As., La Ley, 18/02/2009.

Balardini, Sergio, "Hacia un entendimiento de la interacción de los adolescentes con los dispositivos de la Web 2.0. El caso de Facebook", en Barindelli y Gregorio (comps.), *Datos personales y libertad de expresión en las redes sociales digitales*, Bs. As., Ad-Hoc, 2010.

Baratta, Alessandro, *Resocialización o Control Social. Por un concepto crítico dela "reintegración social" del condenado*, Universidad de Saarland, Alemania, 1993.

Batallanez, Teresa,"La intimidad al desnudo", en revista *La Nación*, Bs. As., 09/01/2011.

Bergalli, Roberto; *Control social punitivo. Sistema penal e instancias de aplicación (Policía, Jurisdicción y Cárcel)*, Barcelona, M. J. Bosch, 1996.

Binder, Alberto, "La fuerza de la inquisición y la debilidad de la república", en *La implementación de la nueva justicia penal adversarial*, Bs. As., Ad-Hoc, 2012.

Binder, Alberto, "Elogio de la audiencia oral", material de lectura otorgado por el Centro de Estudios de Justicia de las Américas (CEJA) en el marco del Programa Argentino de Capacitación para la Implementación de la Reforma Procesal Penal, 2013.

Binder, Alberto, "La fuerza de la oralidad", en *La implementación de la nueva justicia penal adversarial*, Bs. As., Ad-Hoc, 2012.

Binder, Alberto, *Introducción al Derecho Procesal Penal*, Bs. As., Ad-Hoc, 1993.

Cancio Meliá, Manuel, "Una nueva reforma de los delitos sexuales contra la libertad", en *La Ley Penal*, n° 80, año VIII, marzo 2011.

Candarle, Gisela, "Hacia la justicia digital en la Ciudad de Buenos Aires", [en línea] *elDial.com*, DC167D.

Carballeda, Alfredo; *La intervención en lo social. Exclusión e integración en los nuevos escenarios sociales*, Bs. As., Paidós; 2002.

Carnevale, Carlos A., "¿Es posible ser condenado penalmente por descargar música de Internet? —Mp3, P2P y garantías constitucionales—", [en línea] *elDial.com*, 12/03/08.

Carocca Pérez, Alex, *El nuevo sistema procesal penal*, Santiago, Lexis-Nexis, 2005.

Carrera de Hairabedián, Marcela, "Algunas consideraciones sobre los delitos informáticos", *Foro de Córdoba*, nº 63, pp. 57 y ss.

Cassin, Bárbara, *Googléame. La segunda misión de los Estados Unidos*, trad. de Víctor Goldstein, Bs.As., FCE, 2008.

CEJA, *Reformas procesales penales en América Latina: Resultados del Proyecto de Seguimiento*, Santiago de Chile, CEJA, 2005.

CELS, *El estado de la prisión preventiva en la Argentina*, [en línea] http://www.inecip.org/admin/publicaciones/archivos/INECIP_Prision%20Preventiva_digital3.pdf

Cesario, Roberto, *Hábeas Data. Ley 25.326*, Bs. As., Universidad, 2001.

Cohen, Albert, *Delinquent boys. The culture of the gang Delinquent Boys;* Glencoe, III; The Free Press, sd, 1955.

Creus, Carlos, "El miedo a la analogía y la creación de vacíos de punibilidad en la legislación penal (intercepción de comunicaciones telefónicas y apropiaciones de e-mail)", *JA*, 1999-IV-869.

Cherñavsky, Nora A., "El delito informático", en Javier A. De Luca (coord.), *XI Encuentro de Profesores de Derecho Penal de la República Argentina*, La Ley/UBA/AAPDP, 2013, en prensa.

De Gavaldá y Castro, Rubén, *Ceremonial. Un arte para comprender la vida*, Bs. As., Paidós, 2010.

De la Mata Barranco, Norberto J. y Hernández Díaz, Leyre, "El delito de daños informáticos: una tipificación defectuosa", *Estudios Penales y Criminológicos*, [en línea] http://dspace.usc.es/bitstream/10347/4149/1/07.Mata.pdf

Dessecker, Axel, "Veränderungen im Sexualstrafrecht. Eine vorläufige Bewertung aktueller Reformbemühungen", *Neue Zeitschrift für Strafrecht*, Heft 1/1998.

Díaz Cortés, Lina,"El denominado *child grooming* del art. 183 *bis* del Código Penal: una aproximación a su estudio", Madrid, *Boletín del Ministerio de Justicia de España*, año LXVI, n° 2138, 2012.

Díaz Gómez, Andrés, "El delito informático, su problemática y la cooperación internacional como paradigma de su solución: el Convenio de Budapest", en *Revista Electrónica de Derecho de la Universidad de La Rioja* (REDUR), [en línea] http://www.unirioja.es/dptos/dd/redur/numero8/diaz.pdf

Doueihi, Milad, *La gran conversión digital*, (trad. Julia Bucci), Bs. As., FCE, 2010.

Domínguez Lostaló, Juan C. y Di Nella, Yago, *¿Es necesario encerrar?*, Bs. As., Koyatun, 2007.

Duce, Mauricio y Riego, Cristián, "La reforma procesal penal en Chile. Informe acerca del proceso de reforma al sistema de enjuiciamiento criminal chileno", en *Sistema Acusatorio, Proceso Penal, Juicio Oral en América Latina y Alemania*, Fundación Konrad Adenauer, Caracas, 1995.

Etzioni, Amitai, *Los límites de la privacidad*, (trad. Alexander López Lobo), B de F, Bs. As.-Montevideo, 2012.

Faerman, Juan, *Faceboom. El nuevo fenómeno de masas Facebook*, Bs. As., Ed. B, 2009

Farré Trepat, E., *La tentativa del delito*, Barcelona, Bosch, 1986.

Ferrajoli, Luigi, *Derecho y Razón*, Madrid, Trotta, 2001.

Fillia, Leonardo C.; Monteleone, Romina *et al.*, "*Análisis a la reforma en materia de criminalidad informática al Código Penal de la Nación*", *La Ley*, Suplemento Penal, agosto 2008.

Fontán Balestra, *Derecho Penal. Parte Especial*, actualizado por G. A. C. Ledesma, 16º ed., Bs. As., Lexis-Nexis/Abeledo-Perrot, 2002.

García García-Cervigón, Josefina, "El fraude informático en España e Italia. Tratamiento jurídico-penal y criminológico", [en línea] http://revistas.upcomillas.es/index.php/revistaicade/article/download/357/283

Ghersi, Sebastián, "Violación de secretos y privacidad. Los documentos electrónicos", en *Revista Jurídica La Ley*, 2008-F.

Goffman, E., *Internados*. Bs. As., Amorrortu, 1961.

Gouldner, Alvin, *La crisis de la Sociología Occidental*; Bs. As., Amorrortu, 1973.

Granero, Horacio R., "La sanción de la Ley 26.685 de Expedientes Digitales. El principio de equivalencia funcional y la firma digital", [en línea] *elDial.com* - CC2736

Grasso, Mariana, "Violación de Secretos", en Luis Niño y Stella Maris Martínez, (coords.) *Delitos contra la Libertad*, 2° ed., Bs. As., Ad-Hoc, 2010.

Guarinoni, R., *Derecho, lenguaje y lógica*, Bs. As., Lexis-Nexis, 2006.

Guibourg, Ricardo; Allende, Jorge y Campanella, Elena *Manual de informática jurídica*, Bs. As., Astrea, 1996, § 86.

Habermas, Jürgen, *El futuro de la naturaleza humana*, (trad. por R. S. Carbó), Barcelona, Paidós, 2002.

Heinrich, Manfred, "Strafrecht als Rechtsgüterschutz ein Auslafmodell? Zur Unverbrüchlichkeit des Rechtsgutsdogmas", *Festschrift für Claus Roxin zum 80*, De Gruyter, Berlin, 2011.

Hintze, Susana y Danani, Claudia (coords.), *Protecciones y desprotecciones, la seguridad social en Argentina. 1990-2010*, Editorial UNGS, 2011, sd.

Hirsch, Hans J., "Cuestiones acerca de la armonización del derecho penal y procesal penal en la Unión Europea", en AAVV, *Estudios sobre Justicia Penal. Homenaje al Profesor Julio B. J. Maier*, Bs. As., del Puerto, 2005.

Horvitz Lennon, María Inés y López Masle, Julián, *Derecho Procesal Penal chileno*, t. II, Santiago de Chile, Editorial Jurídica de Chile, 2002.

Huxley, Aldous, *Un mundo feliz*, Bs. As., Sudamericana, 1958.

Iellimo, Marcela, "El caso Wikileaks ¿un planteo de cambio para el orden jurídico internacional?", [en línea] *elDial.com*, DC1522.

Ivoskus, Daniel, *Obsesión digital. Usos y abusos en la red*, Bs. As., Norma, 2010

Jansky, Radomir y Lombaert, Ruben, "Hacia una estrategia europea unificada para combatir la ciberdelincuencia", en *E) NAC. E-newsletter*, [en línea] http://cybex.es

Kanto, Damián, "Privacidad en peligro. Para escuchar conversaciones usan celulares como micrófono", *Clarin.com*, 22/04/1998.

Lezertua, Manuel, "El proyecto de Convenio sobre el Cybercrimen del Consejo de Europa", en *Internet y Derecho Penal*, Cuadernos de Derecho Judicial X-2001, Consejo General del Poder Judicial, Madrid, 2001.

Lo Giudice, María Eugenia, "Con motivo de la sanción de la ley que introduce el 'delito de grooming' en el Código Penal (año 2013)", [en línea] *elDial.com*, DC1C0B

Lopes da Silva, Rita, "Direito Penal e Sistema Informático", en *Revista dos Tribunais*, vol. 4, San Pablo, Brasil, 2003.

Lorenzo, Leticia; Lima Magne, Juan José; Maclean Soruco, Enrique y Lima Magne, Iván, *Manual de Litigación en Audiencias de Medidas Cautelares*, *Asociación Internacional de Juristas*, La Paz, CEJIP, 2009.

Maier, Julio, *Derecho Procesal Penal*, t. II, Bs. As., del Puerto, 2004.

Marco Marco, Joaquín, "Menores, ciberacoso y derecho de la personalidad", en AA.VV, *Ciberacoso: la tutela penal de la intimidad, la integridad y la libertad sexual en internet*, Valencia, Tirant lo Blanch, 2010.

Martínez, Santiago, "La reforma de la ley 26.374, alcances y consecuencias", [en línea] http://www.pensamientopenal.com.ar/node/28064

Moeremans, Daniel, "Protección del e-mail como extensión del derecho a la intimidad", en *Revista Jurídica La Ley*, 2007-E

Molinario, Alfredo, *Los Delitos*, (preparado y actualizado por Eduardo Aguirre Obarrio) Bs. As., TEA, 1996, t. II.

Morales García, Óscar, "Apuntes de política criminal en el contexto tecnológico. Una aproximación a la Convención del Consejo de Europa sobre Cyber-crime", en AAVV, *Delincuencia Informática. Problemas de responsabilidad*, Cuadernos de Derecho Judicial IX-2002, Consejo General del Poder Judicial, Madrid, 2002.

Morillas Cuevas, Lorenzo "Nuevas tendencias del derecho penal. Una reflexión dirigida a la cibercriminalidad", en *Cuadernos de Política Criminal*, nº 94, 2008.

Muñoz Conde, Francisco, *Derecho penal. Parte especial*, Valencia, Tirant lo Blanch, 2013.

Navarro, Guillermo R.; Báez, Julio y Aguirre, Guido, "*Violación de Secretos y de la Privacidad*", en Baigún y Zaffaroni (dirs.), *Código Penal y normas complementarias. Análisis doctrinal y jurisprudencial*, Bs. As., Hammurabi, 2008.

Neumann, Ulfrid, "Alternativas: Ninguna. Sobre la crítica más reciente a la teoría personal del bien jurídico", (trad. Carmen Eloisa Ruiz), *Cuadernos de Política Criminal*, nº 93, 2007.

Nuñez, Ricardo C., *Manual de Derecho Penal. Parte especial*, 2° ed. actualizada por Víctor F. Reinaldi, Córdoba, Marcos Lerner, 1999.

Orwell, George, *1984*, España, Salvat, Editores S.A., 1971.

Ossorio y Florit, Manuel, *Código Penal de la República Argentina*, Bs. As., Universidad, 1979.

Palazzi, Pablo A., *Delitos Informáticos*, Bs. As., Ad-Hoc, 2000.

Palazzi, Pablo A., "Google y el Derecho a la Privacidad sobre las búsquedas realizadas en Internet", *RCE* n° 74, 2006.

Pardo Albiach, Juan, "Ciberacoso: Cyberbullying, grooming, redes sociales y otros peli-

gros", en AA.VV., *Ciberacoso: la tutela penal de la intimidad, la integridad y la libertad sexual en internet*, Valencia, Tirant lo Blanch, 2010.

Pastor, Daniel, "La recodificación penal en marcha. Una iniciativa ideal para la racionalización legislativa", en *Revista Pensar en Derecho*, Bs. As., Eudeba, 2012.

Pavarini, Massimo, *Control y dominación. Teorías criminológicas burguesas y proyecto hegemónico*; Bs. As., Siglo XXI, 2003.

Perron, Walter, "Perspectivas de la unificación del derecho penal y del derecho procesal en el marco de la Unión Europea", en AAVV, *Estudios sobre Justicia Penal. Homenaje al Profesor Julio B.J. Maier*, Bs. As., del Puerto, 2005.

Piccone, Verónica M. y Mangini, Marcelo, "UNASUR en el contexto del regionalismo y los paradigmas de la integración latinoamericana", en *Revista de Derecho Público*, año II, n° 5, Bs. As., Ediciones Infojus, 2013.

Pinti, Enrique, "*1984 es el pasado*", en revista *La Nación*, 26/12/2010.

Reggiani, Carlos, *Delitos Informáticos*, Bs. As., La Ley, 2008-D.

Reischl, Gerald, *El engaño Google*, (trads. H. Piquer y C. Sánchez), Bs. As., Sudamericana, 2009.

Rieutord, Andrés, *El recurso de nulidad en el nuevo proceso penal*, Santiago de Chile, Editorial Jurídica de Chile, 2007.

Riquert, Marcelo A., *Código Penal Comentado de Acceso Libre*, [en línea] http://www.pensamientopenal.com.ar

Riquert, Marcelo A., "Delincuencia informática y control social: ¿excusa y consecuencia?", en *Revista Jurídica*, Facultad de Derecho de la UNMDP, año 6, n° 6, 2011, pp. 67/99.

Riquert, Marcelo A., *Delincuencia Informática. En Argentina y el Mercosur*, Bs. As., Ediar, 2009.

Riquert, Marcelo A., "Ciberacoso sexual infantil ('*cibergrooming*')", [en línea] http://www.pensamientopenal.com.ar/sites/default/files/cpc/art._131_ciber_acoso_sexual_infantil_grooming.pdf

Romeo Malanda, Sergio, "Un nuevo modelo de derecho penal transnacional: el derecho penal de la Unión Europea tras el Tratado de Lisboa", en *Estudios Penales y Criminológicos*, Universidad de Santiago de Compostela, vol. XXXII, 2012.

Rosende, Eduardo, *Derecho Penal e Informática. Especial referencia a las amenazas lógico informáticas*, Bs. As., Di Plácido Editor, 2007.

Rovira del Canto, Enrique, "Ciberdelincuencia intrusiva: hawking y grooming", [en línea] http://www.iaitg.eu/mediapool/67/671026/data/Ciberdelincuencia_intrusiva_hacking_y_grooming_Enrique_Rovira.pdf

Rubio Lara, Pedro, "Acoso sexual de menores por Internet: Cuestiones penales, procesales penales y civiles", en AA.VV., *Ciberacoso: la tutela penal de la intimidad, la integridad y la libertad sexual en internet*, Valencia, Tirant lo Blanch, 2010.

Saez Capel, José y Velciov, Claudia,"Artículo 153 bis", en Zaffaroni y Baigún (dirs.), *Código Penal y normas complementarias. Análisis doctrinal y jurisprudencial*, Bs. As., Hammurabi, 2008, t. V.

Small, Gary y Vorgan, Gigi, *El cerebro digital*, (trad. Roc Filella Escolá), Barcelona, Urano, 2009.

Salt, Marcos, "Criminal procedure law provisions on cybercrime in Latin American regarding their compliance with the Budapest Convention (Argentina, Chile, Colombia, Costa Rica, México, Paraguay and Perú)", [en línea] http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079_d_LATAM_procedurallaw_Dec2011.pdf

Sancinetti, Marcelo, "El fracaso de la explicación del ilícito de la tentativa sobre la base de un 'peligro objetivo'", en *Teoría del delito y disvalor de acción*, Bs. As., Hammurabi, 1991.

Schweizer, Katinka, "Grundlagen der psychosexuellen Entwicklung und 'ihrer Storungen'", *Sexuelle Identität und gesellschaftliche Norm*, Gunnar Duttge, Wolfgang Engel und Barbara Zoll (Hg.), Göttinger Schriften zum Medizinrecht, Bd. 10, Universitätsverlag Göttingen, 2010.

Sibilia, Paula, *El hombre postorgánico*, Bs. As., FCE, 2009.

Silva Sánchez, Jesús, *Aproximación al derecho penal contemporáneo*, 2ª ed., Maestros del Derecho Penal, nª 31, Gonzalo D. Fernández (director), Gustavo Eduardo Aboso (coord.), B de F, Bs. As.-Montevideo, 2010.

Silva Sánchez, Jesús-María (dir.), *Lecciones de Derecho Penal. Parte especial*, Barcelona, Atelier, 2006.

Silva Sánchez, Jesús-María, "La responsabilidad penal de las personas jurídicas en el Convenio del Consejo de Europa sobre cibercriminalidad", en AAVV, *Delincuencia Informática. Problemas de responsabilidad*, Cuadernos de Derecho Judicial IX-2002, Consejo General del Poder Judicial, Madrid, 2002.

Souto, Diego y Peluffo, Vanesa, "Fin de la Falsa Oralidad en la Cámara Criminal y Correccional de la Capital Federal. Nuevos desafíos hacia un sistema penal acusatorio", en *Revista de Derecho Penal y Procesal Penal*, Abeledo-Perrot, 2013.

Tazza, Alejandro y Carreras, Eduardo, "La protección del banco de datos personales y otros objetos de tutela penal", en *Revista Jurídica La Ley, Bs. As.*, La Ley 2008-E.

Torres, Ariel, "¿Es Facebook el próximo Google?", en diario *La Nación*, 09/01/2011.

Vaninetti, Hugo A., "Inclusión del 'grooming' en el Código Penal", Bs. As., La Ley, 2013, AR/DOC/4628/2013.

Vaninetti, Hugo A., "Media sanción del Senado al proyecto de 'grooming'", en Suplemento de Actualidad de *La Ley*, Bs. As., 26/04/2012

Vianna, Túlio , *Fundamentos de Direito Penal Informático*, 1ª ed., Río de Janeiro, Forense, 2003.

Vianna, Túlio, "Dos crimes por computador", [en línea] www.mundojuridico.adv.br, en 16/4/03.

Zaffaroni, Raúl, Alagia, Alejandro y Slokar, Alejandro, *Derecho Penal, Parte General;* Bs. As., Ediar, 2005.

Zaffaroni, Raúl, *Las palabras de los muertos*, Bs. As., Ediar, 2011.

Zaffaroni, Raúl; *Política Criminal Latinoamericana; Perspectivas-disyuntivas*; Bs. As., Hammurabi, 1982.

Zavrsnik, Ales, "*La intervención del sistema de justicia penal en las amenazas a la ciberseguridad: ¿panacea o caja de Pandora?*", [en línea] http://cybex.es

Zugaldía Espinar y Marín de Espinosa Ceballos (dirs.), *Derecho penal. Parte especial*, t. I, Valencia, Tirant lo Blanch, 2011.

Índice Temático

E

G

I

L

M

N

P

R

S

T

V

Este libro con una tirada de 10.000 ejemplares, se terminó de imprimir en
los Talleres Gráficos de la Cooperativa Campichuelo Ltda. en mayo de 2014.

GRAFICA
CAMPICHUELO
Cooperativa Obrera Gráfica Campichuelo Ltda

Campichuelo 553 - C.A.B.A. - C1405BOG - Telefax: 4981-6500 / 2065-5202
campichuelo@cogcal.com.ar - www.cogcal.com.ar