Acceso ilegítimo a banco de datos personales, revelación ilegítima de su información e inserción ilegítima de datos (art. 157 bis, CP)

POR **MARCELO A. RIQUERT**

Sumario: 1. Introducción. — 2. Antecedentes. — 3. Tipo objetivo. — 4. Tipo subjetivo. 5. Iter criminis. — 6. Concurrencias. — 7. Pena. — 8. Acción penal.

1. Introducción

La actual redacción del art. 157 bis corresponde a la fijada por ley 26.388 (1), que produjo una masiva actualización del texto del Código Penal con relación a conductas vinculadas a lo que, generalmente, se llama delincuencia informática. Pablo A. Palazzi lo sistematiza bajo la designación de "delitos relacionados con la protección de datos personales" (2), mientras que Marco A. Terragni, en forma simplificada, lo llama "protección de bancos de datos personales" (3).

En este caso particular, el legislador vino a reflejar la preocupación vigente en torno a brindar un adecuado marco de protección penal a la intimidad y la privacidad, lo que se concretó no sólo en las diversas figuras contenidas en la norma en comentario, sino también en otras. Como resalta José Sáez Capel, con el avance de la informática no sólo es más difícil controlar la difusión de datos personales, sino también asegurar la exactitud de aquellos que se almacenan o transmiten para diversos fines (4). De manera concordante, Palazzi señala que hoy día los bancos de datos personales conforman un vasto universo de información donde la mayor parte de nuestras actividades cotidianas quedan rutinariamente registradas y que la evolución tecnológica en lo relativo al tratamiento de tales datos en las últimas tres décadas ha sido tal que fue necesario aprobar normas especiales para regular el fenómeno (5).

Aquel interés entonces fue exteriorizado con elocuencia en los fundamentos de uno de los proyectos que se tuvieron en cuenta para delinear lo que, en definitiva, se consagró como ley 26.388, el de los senadores Rubén H. Giustiniani y Vilma L. Ibarra, donde sostenían que la "reforma legislativa debe desarrollarse teniendo como única mira el respeto a la intimidad garantizado por nuestra Constitución Nacional, evitando cualquier intromisión de terceros que pueda dar lugar a la sociedad vigilada y controlada descripta por George Orwell. Tal obligación de preservar la confidencialidad e inviolabilidad de las telecomunicaciones tienen una un claro raigambre constitucional sustentado por los arts. 18, 19 y 33 de nuestra ley fundamental". Complementando esta apreciación, puede citarse en modo concordante lo señalado por Feldstein de Cárdenas y Scotti en cuanto resaltan que "Vivir en una sociedad en que la información ha evolucionado hasta el punto de erigirse en una suerte de herramienta básica para optimizar la producción de bienes y servicios,

(1) B.O. del 25/6/08. Su artículo 8° es el que dispone la incorporación del art. 157 bis al Código Penal.

(2) En su obra Los delitos informáticos en el Código Penal. Análisis de la ley 26.388, ed. Abeledo-Perrot, Bs. As., 2009, pág. 129.

(3) En su obra Tratado de Derecho Penal, Ed. La Ley, Bs. As., 2012, Tomo II "Parte Especial-1", pág. 551.

(4) Cf. su obra El llamado delito informático no existe, Sucre, Bolivia, 2014, pág. 163. Destaca allí la importancia como precedente que tuvo en el ámbito europeo el "Convenio para la protección de las personas con respecto al tratamiento automático de datos de carácter personal", firmado en Estrasburgo el 28/1/1981 —por eso, en síntesis, "Convenio de Estrasburgo"-, que estableció un estándar protectivo mínimo garantizador de la intimidad que los Estados-parte podrían ampliar (ob. cit., pág. 180).

(5) Ob. cit., pág. 129.

impone la necesidad de proteger el derecho a la intimidad de las personas" (6).

El texto vigente es el siguiente:

ARTÍCULO 157 bis. *"Será reprimido con la pena de prisión de un mes a dos años el que:*

1. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales;

2. Ilegítimamente proporcionare o revelare a otro información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley.

3. Ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales.

Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de un a cuatro años"

Pasamos a analizar, iniciando por sus antecedentes locales y comparados, con la descripción de sus distintos supuestos típicos.

2. Antecedentes

a) Normativos nacionales

1. Ley de Protección de Datos Personales: en el año 2000, la Ley Nº 25.326 (7) de Protección de Datos Personales (reglamentaria del proceso constitucional de Hábeas Data, art. 43 C.N.) había incorporado al Código Penal dos nuevos tipos, el 117 bis dentro del Título II correspondiente a los "Delitos contra el Honor" y el art. 157 bis en el capítulo III de la "Violación de secretos" del Título V "Delitos contra la Libertad".

Este último decía:

"Será reprimido con la pena de prisión de un mes a dos años el que: 1º. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos accediere, de cualquier forma, a un banco de datos personales; 2º. Revelare a otro información registrada en un banco de datos personales cuyo secreto estuviera obligado a preservar por disposición de una ley. Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de uno a cuatro años".

A diferencia del derogado art. 117 bis (8) ("Falsedad en archivos de datos personales y suministro de información falsa"), no se observaban en principio objeciones en cuanto a su ubicación sistemática, ya que las conductas tipificadas en la figura se relacionaban directamente con la violación de secretos en general.

El cotejo con la norma vigente permite advertir que: a) el monto de pena conminado en abstracto es el mismo en lo básico, pero varía la situación del funcionario público que antes podía recibir una inhabilitación que la redacción permitía fuera de un mínimo de dos meses y ahora éste es de un año (y hasta cuatro, por lo que en el máximo, en definitiva, no hay cambio); b) el inciso primero se ha mantenido pero sufriendo algunos cambios de los que nos ocuparemos de inmediato; c) se eliminó el tipo del inciso segundo, aunque algo de la figura se puede considerar recoge el inciso segundo del art. 157 bis, que prevé el proporcionar información de un archivo o banco de datos personales, según ya vimos; d) desapareció la circunstancia calificante del inciso tercero, largamente criticada en función de que su articulación con el inciso primero posibilitaba la interpretación acerca de la extensión del tipo como la inadecuada recepción de una figura de peligro abstracto.

Es claro entonces que se valora positivamente no sólo el apartamiento de la redacción consagrada por la LPDP Nº 25.286, sino también la

(6) Feldstein de Cárdenas, Sara L. y Scotti, Luciana B., "Internet, comercio electrónico y derecho a la intimidad: un avance de los tribunales argentinos", pub. en la biblioteca jurídica online "elDial.com", suplemento de Derecho Internacional Privado y de la Integración, edición del mes de octubre de 2007, sección Doctrina.

(7) 2/11/00.

(8) Su texto era el siguiente: "1º. Será reprimido con la pena de prisión de un mes a dos años el que insertara o hiciera insertar a sabiendas datos falsos en un archivo de datos personales.2º. La pena será de seis meses a tres años, al que proporcionara a un tercero a sabiendas información falsa contenida en un archivo de datos personales.3º. La escala penal se aumentará en la mitad del mínimo y del máximo, cuando del hecho se derive perjuicio a alguna persona.4º. Cuando el autor o responsable del ilícito sea funcionario público en ejercicio de sus funciones, se le aplicará la accesoria de inhabilitación para el desempeño de cargos públicos por el doble del tiempo que el de la condena".

ubicación sistemática. Había sido una crítica de alto consenso que, conforme a su radicación en sede de "Delitos contra el honor" y descripción típica, se penaba el insertar o hacer insertar datos falsos aun cuando nadie se perjudicara (ya que el inc. 3° consideraba esta situación como agravante con la consecuencia ya mencionada para el inc. 1°) y, además, de cara al bien jurídico protegido (honor, en su vertiente objetiva) podría darse el caso que el dato falso no lo lesionara ni lo pusiera en peligro. Incluso, podría pasar lo contrario, es decir, que el dato falso mejorara su crédito o fama.

2. Anteproyecto de 2006: sin ir más lejos, justamente en función de una interpretación acotada del tipo en función del bien jurídico, se explicaba en los fundamentos de este "Anteproyecto de reforma y actualización integral del Código Penal", que se optaba por suprimir al art. 117 bis. Fue elaborado por la Comisión designada por Resoluciones del Ministerio de Justicia de la Nación N° 303/04 y 136/05 y coordinada por el Dr. Alejandro W. Slokar, cuya exposición de motivos decía en el considerando XII: *"Se ha modificado el Capítulo sobre violación de secretos que ahora se denomina "Violación de Secretos y de la privacidad". De este modo, se actualiza la normativa a los nuevos desarrollos tecnológicos e informáticos y se tipifican lesiones intolerables a la privacidad, mediante la utilización de artificios de escucha, transmisión, grabación o reproducción de imágenes o sonido"* (9).

En específico; se agregaba en sus "Fundamentos": *"Se decidió suprimir el artículo 117 bis por su flagrante inutilidad, ya que por más que se inserten falsedades en los bancos de datos personales, si no existe lesión al honor, no se verificará la tipicidad y, si existe tal lesión, el hecho no dejará de ser una injuria, una calumnia, una publicación o reproducción de las vertidas por un tercero o, bajo ciertas condiciones, un delito previsto como violación de secreto o de la privacidad (art. 146, segunda parte)"* (10).

En definitiva, se efectuaba la supresión de la figura y se la fusionaba en un nuevo artículo, el 146, con lo que se advierte clara la coincidencia en el camino seguido por el legislador en la ley que se indica en el punto siguiente.

3. Ley 26.388: menos de una década después de la LPDP, la 26.388, por su art. 3° comenzó sustituyendo el epígrafe del capítulo citado, que pasó a ser el siguiente: "Violación de Secretos y de la Privacidad". Reprodujo con ello, como se adelantó, la misma propuesta que contenía el "Anteproyecto" de 2006. En el art. 14 dispuso la derogación del criticado art. 117 bis del digesto sustantivo. Además, los arts. 7 y 8, sustituyeron los textos de los arts. 157 y 157 bis, recibiendo este último en su nuevo inc. 3° parcialmente la conducta antes reprimida en el inc. 1° de la norma derogada citada.

4. Anteproyecto de Código Penal de 2014: elaborado por la Comisión designada por Decreto del PEN N° 678/12, presidida por el Dr. E. Raúl Zaffaroni. En él se prevé dentro del Capítulo III "Violación de comunicaciones y de la privacidad", en el Título IV "Delitos contra la Libertad", el tipo de "acceso ilegítimo a información" (art. 123) contiene e, incluso, amplía conteniendo otros supuestos de tipicidad vigente (así, el art. 153 bis) o de nueva factura (referencias a datos financieros y confidenciales o el caso de sustitución de identidad). En efecto, son los primeros tres apartados del inc. 3° los que, estrictamente, reproducen el actual texto del art. 157 bis (11). Su texto dice:

"1. Será reprimido con mula de diez a cien días, el que a sabiendas accediere por cualquier medio,

(9) En el medio digital puede encontrarse la versión oficial del texto en la siguiente dirección: http://www.jus.gov.ar/guia/eontent_codigo_penal.htm. También fue publicada en los sitios web Pensamiento Penal (www.pensamientopenal.com.ar) y Derecho Penal Online (www.derechopenalonline.com.ar), que incluso elaboraron en aquel momento sendos foros de discusión al respecto, con amplia concurrencia e interesantes observaciones. En papel, puede consultarse en la sección "Actualidad" de la Revista Nova Tesis de Derecho Penal y Procesal Penal, dirigida por Chiara Díaz y Erbetta, N° 1, Rosario, 2007, pág. 197 y ss. La cita corresponde a esta última, pág. 225. Entre los comentaristas de la ley 26.388, ha sido común el reconocer como un acierto la referida ampliación del epígrafe. Así, Palazzi en "Análisis de la Ley 26.388 de reforma al Código Penal en materia de delitos informáticos", pub. en Revista de Derecho Penal y Procesal Penal, dirigida por D'Alessio y Bertolino, LexisNexis, Bs. As., N° 7, 2008; y Cherñavsky, en "Espionaje electrónico", pub. en la biblioteca jurídica online elDial, número especial del 23/10/08, punto 4 (disponible en http://www.eldial.com.ar; ref.: DCF6B).

(10) Cf. considerando XI in fine de los Fundamentos, pub. en la sección "Actualidad" de la Revista Nova Tesis de Derecho Penal y Procesal Penal, dirigida por Chiara Díaz y Erbetta, N° 1, Rosario, 2007, pág. 224.

(11) Lo reconoce expresamente la "Exposición de Motivos", véase en Anteproyecto de Código Penal, ed. INFOJUS, Bs. As., marzo de 2014, pág. 194.

sin autorización o excediendo la que poseyere, a un sistema o dato informático de acceso restringido.

2. La pena será de seis meses a dos 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 años.

3. Será penado con prisión de seis meses a dos 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 a cinco años" (12).

Sobre el particular, Carlos Christian Sueyro ha observado con razón que el Anteproyecto, en lugar de mantener la figura de acceso ilegítimo a un sistema informático en forma disgregada en tres artículos, se decidió a unirlos en uno solo con cuatro parágrafos o incisos (13).

b) Derecho comparado regional (Mercosur)

Sin perjuicio de centrar la información en lo concerniente al ámbito regional, vale la pena aclarar que en el plano internacional con una perspectiva más amplia, la parte nuclear de esta tipicidad viene propuesta por los arts. 2 y 4 del "Convenio sobre Cibercriminalidad" de Budapest (2001), en los siguientes términos:

Artículo 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*" (14).

Artículo 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,*

(12) Cf. Anteproyecto..., pág. 388.

(13) En su trabajo "La criminalidad informática en el Anteproyecto de Código Penal de la Nación", pub. en AAVV, Informática y Delito, ed. INFOJUS/AIDP Grupo Argentino, Bs. As., 2014, pág. 103.

(14) 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".

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" (15).

González Allonca y Passeron resaltan que las disposiciones del Convenio sobre Cibercriminalidad vinculadas a las actividades de tratamiento de datos personales e informativas en general se encuentran alcanzadas en nuestro país por las disposiciones de la ley 25.326 (ya citada), con manifiesta compatibilidad (16). Sentado ello, comenzando con la comparación suramericana, se divide el artículo en comentario del modo que sigue:

1. Con relación al "acceso ilegítimo a banco de datos personales":

En cuanto al acceso a bancos de datos, en Brasil, con motivo de la incorporación del sistema de voto electrónico en las elecciones de 1996, el año anterior, por ley 9100, art. 67 inc. VII, se introdujo 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, mientras que el inc. VIII 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 (17).

En Bolivia se prevé junto a la alteración y el uso indebido de datos informáticos la punición del acceso a aquellos alojados en una computadora o cualquier soporte informático, en el art. 363 ter (18) de su CP del año 1997.

El C.P. de Colombia (Ley 599 de 2000) ha sido modificado por la Ley 1273 de 2009, que le incorporó como cap. VII bis uno específico para la delincuencia informática, dentro del que el acceso abusivo a un sistema informático está contemplado en el art. 269 (19). Debe tenerse además presente que todas las conductas del capítulo tienen previstas una serie de circunstancia de agravación en el artículo final, el 269 H (20), algunos de cuyos incisos recogen tipicidad análoga al art. 157 bis argentino que se comenta.

---

(15) 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 artículo 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.

(16) Juan C. González Allonca y Ezequiel Passeron, "El Convenio de Budapest sobre Cibercriminalidad y la Ley de Protección de Datos Personales", pub. en la revista Derecho Penal, dirigida por Alagia-De Luca-Slokar, ed. INFOJUS, Bs. As., N° 7, 2014, pág. 54.

(17) Cf. Rita de Cássia Lopes da Silva, Direito Penal e Sistema Informático, Ed. Revista dos Tribunais, Série Ciência do Direito Penal Contemporânea, Vol. 4, San Pablo, Brasil, 2003, págs. 69/70.

(18) 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 informático, ocasionando perjuicio al titular de la información, será sancionado con prestación de trabajo hasta un año o multa hasta doscientos días".

(19) 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 1.000 salarios mínimos legales mensuales vigentes".

(20) 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".

Uruguay ha sancionado el 11 de agosto de 2008 su Ley de Protección de Datos Personales, bajo el Nº 18.331, cuyo artículo 1º 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 (cf. art. 2º). Entre otros principios que rigen la tutela de datos personales está el de reserva (art. 11), enfatizado por la remisión al art. 302 de Código Penal en cuanto a la estrecha guarda del secreto profesional. Precisando quiénes son estos obligados a la guarda de secreto, indica Rubén Flores Dapkevicius que son lo que por su situación laboral u otra forma de relación con el responsable de una base de datos tienen acceso o intervienen en cualquier fase del tratamiento de datos cuando éstos hayan sido recogidos de fuentes no accesibles al público (21). Como organismo de control se crea la "Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento" (AGESIC), en su art. 31, a cuyo cargo está la potestad sancionatoria administrativa (art. 35).

En Venezuela, en el capítulo III "De los delitos contra la privacidad de las personas y de las comunicaciones" de la LECDI de 2001, hay 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) (22) o la violación de la privacidad de las comunicaciones (art. 21) (23).

(21) En su trabajo "La nueva Ley de Habeas Data en Uruguay. Ley Nº 18.331", pub. en Alfa-Redi. Revista Electrónica de Derecho Informático (www.alfaredi.org), Nº 124, noviembre de 2008.

(22) 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".

(23) 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.

2. Con relación al tipo de "proporcionar o revelar ilegalmente información registrada secreta":

En Brasil, mediante la Ley 9983 del año 2000, se introdujo un tipo de violación de secretos calificado por vía de la modificación de los arts. 153 y 325 del CPB. En efecto, el art. 153, parág. 1º, 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. I y 2, "Violación de secreto funcional", prevé pena de detención de 6 meses a 2 años o multa, para el que permite o facilita, 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 se utilizare, indebidamente, de acceso restringido. Califica por daño a la Administración Pública o a otro, con pena de reclusión de 2 a 6 años y multa.

Siempre en el marco de los delitos contra la administración pública, informa Hélio Santiago Ramos Júnior, la ley citada agregó al CPB los arts. 313-A y 313-B, 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. El primero de los tipos mencionados pena con reclusión de 2 a 12 años y multa la conducta de insertar o facilitar, el funcionario autorizado, la inserción de datos falsos, alterar o excluir indebidamente datos correctos en los sistemas informatizados o bancos de datos de la Administración Pública con el objetivo de obtener ventaja indebida para sí o para otra persona o para causar daño (24).

Se trata entonces de un delito "especial" o "propio", en el sentido de requerir una calidad personal en el autor, ser el funcionario público autorizado para la manipulación de los datos del sistema o

(24) Ramos Júnior, en su trabajo "Delitos cometidos contra la Seguridad de los Sistemas de Informaciones de la Administración Pública Brasileña", pub. en Alfa-Redi. Revista de Derecho Informático (www.alfaredi.org), Nº 115, febrero de 2008, sección "Delitos y TICs", punto 1 "Delito de inserción de datos falsos en sistemas de informaciones de la administración pública".

banco de datos público. Aclara el autor nombrado la posibilidad de participación de un tercero sin tal calidad en términos del art. 29 del CPB, sea en coautoría, instigación o alguna modalidad de facilitación, citando en igual sentido las opiniones de Mirabete y Jesús.

A su vez, la segunda norma apuntada tipifica también como delito propio la modificación o alteración no autorizada de sistemas de información. En efecto, asigna pena de detención de 3 meses a 2 años y multa para el funcionario que modifique o altere sistemas de informaciones o programa de informática sin autorización o solicitud de autoridad competente. La pena será aumentada de una tercera parte hasta la mitad en caso de resultar daño para la Administración Pública. Destaca Ramos Júnior que, no obstante tratarse también de un delito de funcionario, el art. 313-B admite un mayor espectro de autores que el art. 313-A, ya que sería posible su comisión por cualquier funcionario (25). En ambos casos, son tipos dolosos.

En el caso de Venezuela, dentro del capítulo III "De los delitos contra la privacidad de las personas y de las comunicaciones" de la LECDI de 2001, encontramos el tipo de revelación indebida de data o información de carácter personal (art. 22) (26).

3. Con relación a la "inserción ilegítima de datos personales":

En Brasil, no hay norma análoga, pero sí se verifica una creciente preocupación por la protección de estos aspectos. Así, como destaca Salete Oro Boff, su legislación acompañó la tendencia del derecho comparado y, a partir de 1988, pasa a contemplar la protección de la vida privada y a la intimidad en un dispositivo específico en el texto constitucional (el art. 5º, X), que considera como inviolables la intimidad, la vida privada, la honra y la imagen de las personas, asegurando el derecho a la indemnización por el daño material o moral procedente de su violación (27). Hace hincapié la nombrada en que el propio texto constitucional trató de reforzar su efectividad al atribuirle aplicación inmediata, tratándose de la atribución de la calidad de cláusula pétrea y, por tanto, no sujeta a la modificación por enmiendas (28). El mismo art. 5, LXXII de la Constitución Federal introdujo el hábeas data para asegurar el conocimiento de las informaciones relativas a la persona accionante que consten en los registros o bancos de datos de entidades gubernamentales o de carácter público (29).

Además, como destaca Rita de Cássia Lopes da Silva, el legislador de 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 arts. 72 y 73 del Código de Defensa del Consumidor, Ley 8079/90. El primero pena 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 (30).

A su vez, en Paraguay, el Código Penal de 1997, con previsiones más cercanas a las de Brasil (a las que preceden) que a las argentinas, al regular los delitos patrimoniales incorporó un tipo de alteración de datos (art. 174). Su texto es el siguiente: *"Artículo 174.- Alteración de datos. 1º 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. 2º En estos casos, será castigada también la tentativa. 3º Como datos, en el sentido del inciso 1º, se entenderán sólo aquellos*

(25) Trabajo antes citado, punto 2.

(26) 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 artículos 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".

(27) El texto original dice "a intimidade, a vida privada, a honra e a imagen das pessoas, assegurando o directo à indenização pelo dano material ou moral decurrente de sua violação".

(28) Selene Oro Boff, "Vida privada e intimidad en la Internet: entre la libertad y la vulnerabilidad", pub. en la Revista de Derecho Nova Tesis, Rosario, 2007, Nº 6, págs. 9/10.

(29) Cf. Rita de Cássia Lopes da Silva, ya citada, pág. 68.

(30) Ya citada, págs. 68/69.

que sean almacenados o se transmitan electrónica o magnéticamente, o en otra forma no inmediatamente visible".

En la "Exposición de Motivos" del propio Código, al referirse a la inclusión del tipo transcripto (y del siguiente, que prevé el sabotaje de computadores), se señala que: "*Dada la creciente importancia que tienen la transmisión de datos y las computadoras en la vida cotidiana y en los negocios que se llevan a cabo en la sociedad, y tomando en cuenta el valor patrimonial que actualmente tiene toda información, es menester que el nuevo código penal posea entre sus previsiones, las herramientas eficaces que permitan la sanción de quienes alteraren datos o sabotearen computadoras, ya sea alterando o borrando la información, así como la destrucción de unidades de almacenamiento (discos duros, diskettes, cd rom), o partes accesorias vitales (tarjetas u otro componente del hardware) que imposibiliten el procesamiento de estas informaciones".*

A su vez, se han dedicado 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 art. 174, antes citado. Se trata de los artículos 248 y 249. Su texto es el siguiente: "*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 artículo 174, inciso 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 artículo 246, inciso 4°" y "Artículo 249.- Equiparación para el procesamiento de datos. La manipulación que perturbe un procesamiento de datos conforme al artículo 174, inciso 3°, será equiparada a la inducción al error en las relaciones jurídicas".*

En Perú, la alteración, daño y destrucción de base de datos, se había incorporado al C.P. de 1991 por ley 27.309 (17/7/00), como nuevo art. 207-B, que también recibía los agravantes del art. 207-C. Fueron derogados por la "disposición complementaria derogatoria única" de la ley 30.096 de 2013, cuyo art. 3 "Atentado contra la integridad de datos informáticos" es el tipo actualmente regente (31).

3. Tipo objetivo

a) Bien jurídico

Buompadre sostiene que estos delitos protegen la intimidad personal, entendida como espacio de reserva de los individuos necesario para el desarrollo de la personalidad y que el Estado debe preservar de toda intromisión ilícita por parte de personas no autorizadas (32). Aboso coincide en que el bien jurídico tutelado sigue siendo la intimidad de las personas pero puntualiza, en especial, que lo son los datos personales almacenados en un sistema informático y aclara que no excluye la afectación del servicio informático en sí "pero lo importante acá es proteger el uso extendido de los ordenadores en la vida cotidiana y el proceso de tratamiento y almacenamiento de la información ajena contenida en bancos de datos" (33).

Entendemos que, como enseñaba el maestro Núñez, lo protegido en este capítulo del Código Penal era la incolumidad de: a) la intimidad de la correspondencia y de los papeles privados y, b) los secretos y la libre comunicación entre las personas (34). Hemos en otra oportunidad señalado que, en función de la anterior reforma, se pasó a incluir: c) la información que se hallare registrada en un banco de datos personales, que se conecta con el primer aspecto (intimidad) en el inciso 1° del art. 157 bis y el segundo (secreto) en el inc. 2°, tratándose desde el punto de vista del autor de un delito común que preveía como agravante la realización por funcionario público (35).

(31) 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".

(32) Jorge E. Buompadre, Manual de Derecho Penal. Parte Especial, Astrea, Bs. As., 2013, pág. 379.

(33) Gustavo E. Aboso, Código Penal de la República Argentina. Comentado, concordado con jurisprudencia, ed. B de F, Montevideo/Buenos Aires, 2012, pág. 780.

(34) Ricardo C. Núñez, Manual de Derecho Penal. Parte Especial, Marcos Lemer Editora Córdoba, 2ª edición actualizada por Víctor F. Reinaldi, 1999, pág. 175.

(35) Así, en Riquert, Delincuencia informática en Argentina y el Mercosur, Ediar, Bs. As., 2009, pág. 114.

Según se detalló en los antecedentes, ahora se ha incluido en el epígrafe del capítulo la "privacidad" en forma expresa, lo que evita la necesidad de cualquier tipo de construcción como la anterior para dotar de sentido a la ubicación de la figura e interpretarla adecuadamente. Coinciden en la bondad de la inserción Navarro, Báez y Aguirre, diciendo que *"Este agregado es adecuado pues, como se verá, no todo lo protegido es secreto sino simplemente privado, es decir que su conocimiento es exclusivo para el destinatario"* (36). En definitiva, se trata de una versión complejo del objeto de protección que no debiera reconducirse sólo a la "intimidad" en sentido lato.

Terragni coincide en cuanto plantea que no se trata sólo de evitar la revelación de secretos, sino que comprende en general la intimidad pero no únicamente en su inteligencia como prerrogativa excluyente de terceros respecto de determinados ámbitos de la vida privada, sino también en cuanto se la concibe como un derecho de control sobre la información y los datos de la propia persona, incluso sobre los ya conocidos, para que sólo puedan utilizarse conforme a la voluntad de su titular (37). Por eso, concluye que la protección de datos propuesta por la norma en estudio va de la mano con los derechos de tercera generación, que desde 1994 integran nuestra Constitución Nacional dentro del Título de los "Nuevos Derechos y Garantías" (38).

Finalmente, debe agregarse que la protección de datos personales ha sido complementada en la órbita contravencional por medio de la disposición 1/2003 (39) de la Dirección Nacional de Protección de Datos Personales (autoridad de contralor de la ley de Hábeas Data).

b) Verbo típico

Con relación al inciso primero (acceso ilegítimo o no autorizado a banco de datos personales), se advierte que la redacción conforme a la ley 26.388 es idéntica a la anterior, al igual que el monto de la pena conminado en abstracto y la circunstancia calificante de autoría por un funcionario público. La acción típica de acceder, es decir, penetrar, ingresar o introducirse, lo que /conforme aclara Buompadre- implica que la conducta típica no puede tener cabida en la etapa de recogida de datos, sino que demanda que estos ya estén incorporados, almacenados, en el sistema informático (40). Puede concretarse por cualquier medio ya que no se especifica modalidad de ingreso alguna, aunque el contexto de la reforma es claro en cuanto a que el legislador quiso referirse a los medios informáticos (41).

Teniendo en cuenta el bien jurídico protegido, Buompadre postula que el acceso implica la toma de conocimiento de los datos, no bastando el mero ingreso clandestino al sistema sin imponerse del contenido de la información ya que sólo mediante esto último podría afectarse la intimidad personal del titular del dato (42). Sin embargo, parece soslayar que en realidad el afectado por la conducta es el titular del banco de datos que con el mero acceso ve violentado el secreto que debe presidir la recolección, preservación y procesamiento de datos.

Respecto al inciso segundo, realizado el cotejo entre los distintos textos de este artículo trans-

(36) Guillermo R. Navarro, Julio C. Báez y Guido J. Aguirre, en su comentario al "Artículo 153", pub. en AAVV, Código Penal, dirigido por David Baigún y Eugenio R. Zaffaroni, ed. Hammurabi, Bs. As. Tomo 5, 2008, pág. 711.

(37) Ob. cit., pág. 551.

(38) Ob. cit., pág. 552.

(39) Pub. en el B.O. del 30/6/03. Fuente: Diario Judicial, sección Noticia del Día, correspondiente al 30 de junio de 2003 (www.diariojudicial.com.ar). Mediante ella se aprobó la "clasificación de infracciones" y "la graduación de sanciones" a aplicar frente a las infracciones que atenten contra la LPDP. Entre los objetivos perseguidos con ello, las autoridades han señalado que la disposición obedece a razones de seguridad jurídica, ello en un marco de acciones que tienen como norte la prevención, la difusión y educación de los ciudadanos sobre la protección de los datos personales. La normativa dictada dispone una clasificación de infracciones con sus pertinentes escalas sancionatorias. Las categoriza en leves (desde $ 1000 a $ 30.000), graves ($ 3.000 a $ 50.000) y muy graves ($ 50.000 a $ 100.000).

(40) Cf. Buompadre, ob. cit., pág. 379.

(41) Cctes.: De Langhe, Marcela — Rebequi, Julio M.: comentario al "Artículo 157 bis", pub. en AAVV Código Penal, dirigido por David Baigún y Eugenio R. Zaffaroni, ed. Hammurabi, Bs. As. Tomo 5, 2008, pág. 815; Donna, Derecho Penal. Parte Especial, Rubinzal-Culzoni Editores, Santa Fe, 2001, pág. 380. Allí relaciona la figura con la del art. 197.2 del CPE, con cita a Polaino Navarrete en el sentido que todo acceso cognitivo no autorizado al banco de datos reservados implica una lesión del bien jurídico "intimidad", garantizado al titular de aquéllos.

(42) Ob. cit., pág. 379.

criptos el inicio y en los antecedentes, el vigente ofrece algunas diferencias con el precedente. Así, no contempla sólo la conducta "revelare", sino también "ilegítimamente proporcionare", además de que la información registrada puede no estarlo sólo en un banco de datos personales, sino en un simple "archivo", lo que le permite aprehender un universo mayor de casos, una mayor variedad de conductas.

En cuanto al significado de "revelar", importa el dejar ver, mostrar o exponer a otro la información que se debe mantener en secreto, es decir, destaparla o descubrirla, correr el velo permitiendo que se conozca; mientras que "proporcionar" es la acción de "hacer lo necesario para que una persona tenga algo que necesita, facilitándoselo o dándoselo" (43). Destaca Buompadre que esta facilitación o puesta a disposición puede concretarse por cualquier medio, informático o no, oral o escrito (44).

En estos términos, queda claro que mientras el primer inciso pena el "acceso" por parte de cualquiera, aquí se lo hace respecto del revelar o proporcionar ilegalmente los datos a un tercero por parte de quien tiene la obligación de guardar secreto. Amans y Nager señalan que se trataría de una modalidad específica del convencional delito de violación de secretos, generada por los avances tecnológicos (45).

Finalmente, el inciso 3° que recoge parcialmente una tipicidad que estaba en el art. 117 bis derogado (sede de delitos contra el honor), pena la ilegítima inserción de datos en un archivo de datos personales. "Inserta" quien incluye datos en el archivo de datos personales, mientras que "hace insertar" quien logra que un tercero los introduzca. La otra persona no necesita participar dolosamente, puede que lo haga engañada, por error, en cuyo caso —apunta Terragni— configuraría un supuesto de autoría mediata (46).

Amans y Nager apuntan que se debería además requerir que tal inserción tenga virtualidad suficiente para producir la lesión del bien jurídico, por lo que entienden que no cualquier inserción es suficiente para configurar el injusto (47). Por su lado, Buompadre resalta que debe tratarse de datos personales, careciendo de relevancia que sean falsos o verdaderos, que sean de terceros o del propio titular (48). También Terragni enfatiza la suficiencia de la incorporación ilegítima, sin que el tipo exija que los datos insertados sean falsos (49).

c) Elementos

La insistente señalización de ilegitimidad en cada uno de los incisos de la norma analizada constituye un elemento normativo que viene a enfatizar la falta de consentimiento (50). Lógicamente, de contar con éste no estaríamos frente a una conducta punible. Las reglas vinculadas al consentimiento, a la cesión de datos y distintas situaciones posibles vinculadas a supuestos especiales, se especifican en la LPDP (25.326).

La redacción ha sido justamente criticada por redundante ya que si se violan sistemas de confidencialidad, con evidencia se lo hace a sabiendas y careciendo de derecho (51). No obstante, observan De Langhe y Rebequi que la incorporación del elemento normativo "ilegítimamente" en la redacción vigente lleva por consecuencia singular en la tercera tipicidad que baste la incorporación del dato sin derecho, aunque pudiera ser verdadero (52).

En cuanto a otros elementos del tipo de carácter normativo, sus conceptos básicamente vienen provistos por el art. 2 de la LPDP N° 25.326. Así, nos dice que por "datos personales" ha de enten-

(43) Así, la definición que brinda el Diccionario Enciclopédico Ilustrado Larousse, ed. La Nación, Bs. As., 2005, pág. 945.

(44) Ob. cit., pág. 380.

(45) Carla V. Amans y Horacio S. Nager, Manual de Derecho Penal. Parte Especial, dirigido por Carlos A. Elbert, Ed. Ad-Hoc, Bs. As., 2009, pág. 219.

(46) Ob. cit., pág. 555.

(47) Ob. cit., pág. 219.

(48) Ob. cit., pág. 381.

(49) Ob. cit., pág. 551. En igual sentido, Aboso, ob. cit., pág. 782.

(50) Ccie.: Terragni, ya citado, pág. 553.

(51) Así, De Langhe y Rebequi, ya citados, pág. 816. Ccies.: Palazzi, ya citado, págs. 145/146; Horacio S. Nager, en su trabajo "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", pub. en la revista Derecho Penal, dirigida por Alagia-De Luca-Slokar, ed. INFOJUS, Bs. As., N° 7, 2014, pág. 95.

(52) Ob. cit., págs. 822/823.

derse la información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables; por "datos sensibles" aquellos 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 "datos informatizados" aquellos datos personales sometidos al tratamiento o procesamiento electrónico o automatizado; por "archivo, registro, base o banco de datos", en forma indistinta, el conjunto organizado de datos personales que sean objeto de tratamiento o procesamiento, electrónico o no, cualquiera fuera la modalidad de su formación, almacenamiento, organización o acceso.

d) Sujeto activo

Las distintas hipótesis típicas están redactadas de tal modo que es necesario diferenciar entre ellas ya que median en algún caso restricciones a que cualquiera pueda ser su autor (delito común). En el caso del primero y del tercer inciso, puede ser cualquier usuario no autorizado con la debida clave. Cualquiera que burle la protección dispuesta por el servidor, dice Marco A. Terragni (53).

En el segundo, en cambio, debe tratarse de alguien que esté obligado a preservar el secreto de la información por disposición de la ley. De Langhe y Rebequi destacan que, por ello, el agente es alguien que cubre rol de "garante" de la privacidad, tratándose en definitiva de un delito propio, de autoría especial o de autor calificado (54). En general, el art. 10 de la Ley 25.326 de Protección de Datos Personales, establece el "deber de confidencialidad" en los siguientes términos: "*1. El responsable y las personas que intervengan en cualquier fase del tratamiento de datos personales están obligados al secreto profesional respecto de los mismos. Tal obligación subsistirá aun después de finalizada su relación con el titular del archivo de datos. 2. El obligado podrá ser relevado del deber de secreto por resolución judicial y cuando medien razones fundadas relativas a la seguridad pública, la defensa nacional o la salud pública*".

Volviendo a la norma en comentario, el párrafo final, común a todos los incisos que le preceden, prevé que si el autor fuere un funcionario público le corresponderá además una pena de inhabilitación especial de uno a cuatro años. Entiendo que para habilitar la procedencia de esta circunstancia agravante no basta la objetiva posesión de la calidad personal sino que el ejercicio de la actividad funcional en el marco del hecho atribuido cobra relevancia (55).

e) Sujeto pasivo

En la primera tipicidad resulta ser el titular del banco de datos (persona física o jurídica (56) mientras que, sin perjuicio de ellos, puede entenderse que en todas lo es el titular de los datos reservados que son ilegítimamente accedidos, revelados o modificados por inserciones.

El art. 2 de la Ley 25.326 indica que "responsable de archivo, registro, base o banco de datos" es la persona física o de existencia ideal pública o privada que es titular de un archivo, registro, base o banco de datos; por "titular de los datos" ha de entenderse toda persona física o de existencia ideal con domicilio legal o delegaciones o sucursales en el país, cuyos datos sean objeto del tratamiento al que se refiere la propia ley; mientras que "usuario de datos" es 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 conexión con ellos.

4. Tipo subjetivo

En todos sus incisos estamos frente a conductas dolosas. El giro "a sabiendas" con el que comienza el primero de ellos, es indicativo de que se trata de un supuesto que demanda dolo directo (57).

(53) Ob. cit., pág. 553.

(54) Ob. cit., pág. 821.

(55) En contra: Buompadre, ob. cit., pág. 382; Aboso, ob. cit., pág. 781; Terragni, ob. cit., pág. 555; Carlos Creus y Jorge E. Buompadre, Derecho Penal. Parte Especial, Astrea, Bs. As., 7ª edición actualizada y ampliada, 2007, pág. 405 (con referencia a la redacción conforme a la LPDP, pero válido para el texto vigente).

(56) En contra de la inclusión de la persona jurídica como sujeto pasivo: Terragni (ob. cit., pág. 554).

(57) Ccles.: Buompadre, ob. cit, pág. 380; Amans y Nager, ya citados, pág. 218; Terragni, ob. cit., pág. 554; Nager, ob. cit., pág. 96; Creus y Buompadre, ob. cit., pág. 405 (con referencia a la redacción conforme a la LPDP, pero válido para el texto vigente).

Aun sin él, la tercera hipótesis también luce en principio compatible con esa misma modalidad (58). Palazzi entiende que la norma lleva implícito un dolo especial, que consiste en el conocimiento y la intención de alterar la información personal del titular de los datos personales (sea resultado de un dato falso o verdadero) (59).

En cambio, respecto de la conducta del segundo inciso parece admisible su compatibilidad con el dolo eventual (60).

5. Iter criminis

Con relación a la primera hipótesis típica puede señalarse que, al tratarse de un delito de pura acción o pura actividad, la lesión al bien jurídico protegido se concreta con el mero acceso, no siendo necesaria la verificación de otro resultado autónomo, como podría ser que el agente se apropie de datos que integran el banco (61). Sin embargo, resulta admisible la tentativa ya que es factible que el *iter criminis* sea interrumpido en momentos en que alguien intenta el acceso, por razones ajenas a su voluntad (62).

Respecto a la segunda tipicidad, la lesión al bien jurídico protegido se concreta con la simple revelación o el proporcionar la información (63) y, también en este caso, resulta posible la tentativa (64).

En orden a la tercera hipótesis típica, De Langhe y Rebequi, no obstante considerarla es un delito formal, de peligro abstracto (65), postulan que es admisible la tentativa (66). Buompadre, en cambio, lo considera como de peligro concreto y niega la posibilidad de tentativa por entender que se consuma con la introducción del dato en el archivo de datos personales y es en ese momento que se coloca en peligro de lesión al bien jurídico protegido (67).

Concuerda Aboso en la posibilidad de tentativa en los tres supuestos (68).

6. Concurrencias

No son de descartar posibles concursalidades, siendo la más evidente dentro del mismo capítulo la que mediaría en relación aparente de especialidad entre el primer inciso y el art. 153 bis (acceso ilegítimo simple).

Interesante ejemplo de desplazamiento inverso brinda Palazzi, con el caso de quien accede a un banco de datos que no tiene datos personales, sino sólo estadísticos, supuesto en que no debiera aplicarse el art. 157 bis sino el 153 bis (69). El mismo autor aporta otra buena hipótesis de desplazamiento, en este caso con el art. 155: si la base de datos fuera de correos electrónicos o de otras comunicaciones almacenadas de ese modo y el sujeto activo las revela. Es más, dice Palazzi,

(58) Concuerdan Buompadre, afirmando que concluye en tal sentido inducido por la exigencia de que se obre "ilegítimamente" (ob. cit., pág. 382); Aboso, ob. cit., pág. 782.

(59) Ob. cit., pág. 157. Agrega a renglón seguido: "Dado que la persona espera la fidelidad de sus datos, quien los altera sin permiso del responsable del banco de datos comete el delito previsto en este inciso".

(60) Respecto de la anterior redacción del inciso 2º puntualizaba Donna la posibilidad de realización del tipo con dolo eventual (ob. cit., pág. 381). Ccte.: Nager, ya citado, pág. 97. En contra: Buompadre, que postula sólo admite dolo directo (ob. cit., pág. 381); Aboso, ob. cit., pág. 782.

(61) Cctes.: Ledesma, quien refiriéndose al art. 157 bis 1º párrafo, entiende que es un delito formal o de pura actividad, que se consuma con el solo hecho de acceder, sin necesidad de la divulgación de datos ni de que se cause perjuicio, real o potencial (al actualizar la obra de Carlos Fontán Balestra, Derecho Penal. Parte Especial, 16ª edición, LexisNexis Abeledo-Perrot, Bs. As., 2002, pág. 383); De Langhe y Rebequi, ya citados, pág. 816.

(62) Ccte.: Buompadre, que brinda el ejemplo de quien es sorprendido al ingresar al sistema (ob. cit., pág. 380).

(63) Ccte.: Ledesma, quien en cuanto al 2º párrafo del texto anterior, señalaba que el sujeto pasivo es el titular de los datos revelados que es, según el art. 2º de la ley 25.326, toda persona física o jurídica con domicilio legal o delegaciones o sucursales en el país, cuyos datos sean objeto del tratamiento al que se refiere al propia ley (ob. cit., pág. 385).

(64) En igual sentido se pronuncian De Langhe y Rebequi (ya citados, pág. 820) y Buompadre (ob. cit., pág. 381).

(65) Ccte.: Terragni, ob. cit., pág. 555.

(66) Ob. cit., págs. 822/823.

(67) Ob. cit., pág. 382.

(68) Ob. cit., pág. 783.

(69) Ob. cit., pág. 146.

si existe interés público, hasta podría invocarse la excusa absolutoria allí prevista (70).

También sería factible que alguna modalidad de falsedad documental concurra con el inciso tercero.

7. Pena

Se ha previsto una escala de prisión con mínimo de un mes y máximo de dos años para los tres incisos, con agravante cuando el agente sea funcionario público, caso en el que además tendrá inhabilitación especial de uno a cuatro años. Nora Cherñavsky ha resaltado que el legislador nacional ha optado por penar las infracciones a la privacidad con una escala de 15 días a 6 meses cuando se trata del acceso indebido tanto a correos como a comunicaciones electrónicas (art. 153, CP), como a un sistema informático (art. 153 bis, CP), que asciende o se eleva hasta el mes a los dos años cuando lo es respecto a una base de datos (art. 157 bis, inc. 1°, CP) (71). Es decir que media una diferenciación según lo que se acceda (correo, sistema o banco de datos) y, en el último caso, se observa que mientras que el mínimo se incrementa al doble, el máximo se cuadruplica.

Conforme se expuso al comienzo, el "Anteproyecto" de 2014 está proponiendo mantener el tope en dos años, pero subir el mínimo a seis meses, lo que se explica porque se trata de una decisión político criminal genérica que lo preside de no tener penas privativas de libertad de menos de seis meses, lo que se acompaña de un sistema de penas alternativas que suple o reemplaza lo que hoy son prisiones de corta duración.

8. Acción penal

Ledesma, al referirse a la acción penal entiende que al no haberse modificado el art. 73 del digesto sustantivo por la LPDP incluyendo al art. 157 bis entre las excepciones que contiene, debe entenderse que la acción para perseguir este delito es privada (72), punto en el que entendemos le asistiría razón, ya que la exclusión se refiere taxativamente a los arts. 154 y 157, tratándose de un aspecto que no ha sido abordado en la reforma actualmente vigente (73).

Coincide Nager, enfatizando que más allá de la tesis del olvido legislativo y la opinión de algún sector de la doctrina, una interpretación contraria a lo normado en el art. 73 citado vulneraría el principio de legalidad en perjuicio del eventual inculpado (74). Sin perjuicio de ello, pone de resalto la confusión que se genera porque siendo que el inciso 3° reproduce lo que antes era una tipicidad del derogado art. 117 bis, resulta que cuando estaba radicada en dicha sede la acción era pública (75).

Buompadre, si bien en principio sostiene que la acción es privada, postula que debe diferenciarse conforme al carácter de los datos almacenados en bancos de datos, es decir, distinguiendo según sean públicos o privados y, para el primer caso, entiende que la acción será de naturaleza pública y promovible de oficio (76).

Es que no se trata de un problema menor que ya se ha planteado en numerosas ocasiones y no resulta nada razonable que en casos donde los sujetos activos son funcionarios públicos o cuando se trata de conductas que han tenido por afectados a sistemas informatizados de igual carácter, la acción sea privada. Palazzi recuerda que uno de los casos más comentados antes de la reforma por ley 26.388 se relacionó con el tráfico de una base de datos reservada de la ANSeS con información personal de doce millones de afiliados a obras sociales y beneficiarios de subsidios para desocupados (77), que finalmente, en 2008, terminó siendo anulado porque se trataba el del art. 157 bis de un delito de acción privada y no pública, por lo que el impulso de la causa no debió haber

(70) Ob. cit., pág. 150.

(71) En su conferencia "El delito informático", pub. en AAVV, "XI Encuentro de Profesores de Derecho Penal de la República Argentina. Rosario, junio de 2011", Javier A. De Luca coordinador, ed. UBA/AAPDP/La Ley, Bs. As., 2013, pág. 285.

(72) Ob. cit., pág. 384 (inc. 1°) y 385 (inc. 2°).

(73) Ctes.: Palazzi, ob. cit., pág. 158; De Langhe-Rebequi, ob. cit., pág. 824, donde citan en igual sentido la opinión de Andrés J. D'Alessio, en su Código Penal. Comentado y anotado, ed. La Ley, Bs. As., 2004, tomo II, pág. 374.

(74) Ya citado, pág. 96.

(75) Ya citado, pág. 98.

(76) Ob. cit., pág. 382.

(77) Ob. cit., pág. 146. En la nota al pié N° 163 individualiza el fallo de primera instancia (Dr. Ercolini), confirmado por la CNCyCFed, Sala 1, fechado el 19/10/2006, causa N° 39.397, Reg. 1128.

estado a cargo de un fiscal, sino de la persona o institución damnificada (78).

Señala Eduardo E. Rosende que, para solucionarlo, se presentó a una propuesta a la Comisión que elaboró el "Anteproyecto" de 2014 que, aun cuando no fue tomada textual (79), se recibió parcialmente en forma favorable porque en el art. 44 (acciones privadas) se mantuvo sólo al acceso ilegítimo a información del art. 123 en su inciso 1° (equivalente al actual art. 153 bis) e inciso 3° apartados "a" y "c" (serían los actuales incisos 1° y 3° del art. 157 bis). No obstante comentar positivamente que sólo han quedado "conductas que no giran en relación a la función pública", Rosende llama la atención en torno que "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, sólo podría ser aquel cuya privacidad es afectada por los datos de contenidos en la base y el propietario de la base misma, que debería responder civilmente ante el primero" (80). ◆

(78) Ob. cit., pág. 147. En la nota al pié N° 165 se individualiza el fallo: JNCyCFed N° 7, Sec. 14, causa "P., M", rta. el 7/10/2008.

(79) Véase su trabajo titulado "Los denominados delitos informáticos y la estructura general del Anteproyecto de Código Penal", pub. en la revista Derecho Penal, dirigida por Alagia-De Luca-Slokar, ed. INFOJUS, Bs. As., N° 7, 2014, pág. 186.

(80) Trabajo citado, pág. 187.