Violación de Secretos y de la Privacidad

Por **Ricardo Gutiérrez**, **Laura C. Radesca** y **Marcelo A. Riquert**

Art. 153 BIS[1]**.-** ***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.

1. Antecedentes (genealogía del tipo)

Al igual que en el caso anterior, se comenzará por la presentación de la genealogía típica en el derecho argentino y, además, se brindará un breve paneo sobre el estado actual de la legislación similar en el ámbito regional más inmediato: el Mercosur.

a) Normativos nacionales

a.1. *Anteproyecto de ley la Secretaría de Comunicaciones de la Nación (2001*[2]*):* vale la pena su mención, entre otras razones, por su metodología de elaboración, con una comisión especial cuyo producto quedó abierto en su oportunidad a discusión pública. Se preveía una figura similar al actual art. 153 bis en el art. 1°[3], para la que conminaba con pena en abstracto de multa de mil quinientos a treinta mil pesos. Justamente la sanción es otro aspecto resaltable que, lamentablemente, fue dejado de lado en el texto vigente.

a.2. *Anteproyecto de Ley de Reforma y Actualización Integral del Código Penal (2006):* obviamente, nos encontramos ante una figura penal de nueva factura. Si bien este anteproyecto había

[1] Incorporado conforme art. 5° de la Ley N° 26388.
[2] Pub. en el B.O. N° 29782 del 26/11/01, además del sitio web oficial de la Secretaría.
[3] Su primer párrafo decía: *"Será reprimido con pena de multa de mil quinientos a treinta mil pesos, si no resultare un delito más severamente penado, el que ilegítimamente y a sabiendas accediere, por cualquier medio, a un sistema o dato informático de carácter privado o público de acceso restringido…".*

avanzado en la solución de varios de los vacíos legales denunciados en la legislación penal vinculados a la delincuencia informática, autores como Palazzi criticaban que en su art. 146 se mantuviere la tipificación del acceso ilegítimo a un banco de datos (introducida por Ley 25.326), pero no a la conducta más amplia de acceso a un sistema informático, apuntando que en el año 2005 cerca de 50 países legislaron como delito el acceso no autorizado a sistemas informáticos[4].

Otros, como Rosende, postulaban expresamente en contra de la inclusión de la figura alegando, entre otras cosas, que aún cuando fuera difícil distinguir el caso en que constituyera el acto previo de otros más graves, era posible, y resulta inaceptable suplir deficiencias procesales por vía de incriminar autónomamente la mera intrusión que bien pudiera ser un sencillo caso de comprobación de vulnerabilidades de un sistema informático[5]. Juan Pablo Gallego cuenta entre quienes reclamaban la promoción de un debate sobre si la intrusión en un sistema debía ser penalizada "per se" o si sólo debe serlo en caso de difusión o revelación de datos protegidos o que efectivamente se produjeren daños en el sistema accedido[6].

Por nuestra parte, indicamos la conveniencia de profundizar la discusión sobre una alternativa que entendíamos viable, como la de intentar primero una contención por vía contravencional[7]. Similar temperamento sostenía en el derecho español Esther Morón Lerma, afirmando la inoportunidad de una incriminación autónoma de la conducta del mero intrusismo informático por revelarse como una huida al derecho penal, acudiendo a éste como "prima ratio" sin que mediara el convencimiento de la ineficacia de la tutela administrativa, lo que postulaba como posible e idónea en el marco de la LORTAD, en definitiva, *"una respuesta normativa adecuada frente a los riesgos generados por los accesos inconsentidos"*[8].

En definitiva, con lo anterior queda claro que, más allá de reconocer que en muchos países, como ahora el nuestro, se optó por punir el "hacking" en su forma más sencilla, el grado de consenso sobre la necesidad real de utilizar el derecho penal en estos casos carece de mayoritario consenso.

---

[4] Palazzi, *"Breves comentarios a los proyectos legislativos sobre delitos informáticos"*, pub. en "Revista de Derecho Penal y Procesal Penal", dirigida por D'Alessio y Bertolino, Lexis-Nexis, Bs.As., N° 8, Agosto, 2006, pág. 1531.

[5] Rosende, Eduardo E.: *"El intrusismo informático. Reflexiones sobre su inclusión al Código Penal"*, pub. en AAVV *"Crisis y futuro de la legislación penal"*, AAPDP/Ediar, Bs.As., 2008, págs. 334/335.

[6] Gallego, en su trabajo *"El acceso no autorizado a un sistema informático ante el vacío legal en la materia"*, pub. en "RAP. Revista Argentina del Régimen de la Administración Pública", N° 284, Mayo de 2002, pág. 146.

[7] Entre otros, en Riquert, *"Hacking, Cracking, E-mail y dos fallos judiciales que denuncian lagunas en la legislación penal argentina"*, pub. en la *"Revista Jurídica de Mar del Plata"*, Nº 1, año 2002, Facultad de Ciencias Jurídicas y Sociales de la Universidad FASTA de Mar del Plata, Ed. Gowa, Bs.As., págs. 229/250.

[8] Morón Lerma, *"Internet y Derecho Penal: Hacking y otras conductas ilícitas en la red"*, Editorial Aranzadi, Pamplona, 1999, pág. 140.

Así, incluso autores que postulan la existencia de sólidos argumentos para la represión autónoma de esta conducta, como Nuria Matellanes Rodríguez, reconocen que en ordenamientos jurídicos como el español, la respuesta es vacilante y tímida, apuntando como paradigmática la previsión del Convenio del Consejo de Europa sobre el Cibercrimen, de 23 de noviembre de 2001, *"permitiendo a las Partes escoger entre castigar el mero acceso o interceptación de los datos informáticos de otro sistema informático o el acceso acompañado de ulteriores intenciones delictivas: es decir, en ningún momento impone a las Partes contratantes la obligación de castigar autónomamente el puro intrusismo informático"*[9].

a.3. *Ley 26388 (B.O: del 25/6/08):* como bien destacan José Sáez Capel y Claudia E. Velciov, de la discusión parlamentaria ningún fundamento se desprende sobre esta decisión, tratándose de una figura que carecía de antecedentes y que, concretamente, en sede parlamentaria registraba proyectos donde se la consideraba un acto preparatorio no punible (por caso, el proyecto 0117-S-2000; en igual línea: el citado anteproyecto de 2006), así como otros donde se la penalizaba (proyectos 0064-CD-2002; 3873-CD-2006; 5084-CD-2006 y 5864-CD-2006)[10]. Podemos anotar que, sencillamente, en la presentación de fundamentos del proyecto se aludió a que el acceso ilegítimo se encuentra entre los delitos reconocidos por Naciones Unidas, por lo que se la considera como una figura clásica en el catálogo de delitos informáticos.

b) Derecho comparado regional

Recordamos que la reforma introducida por Ley 26388, en general, ha servido no sólo para actualizar el Código, sino para acercar nuestra legislación interna a las demandas del *"Convenio sobre Cibercriminalidad"* de Budapest (2001) en materia fondal. La nueva redacción acordada a nuestro art. 153 bis permite cubrir la tipicidad reclamada por el art. 2[11]. Es interesante resaltar que si bien el Convenio toma partido por considerar delito el simple "hacking", permite que los signatarios introduzcan condicionantes tales como la vulneración de medidas de seguridad y elementos

[9] Matellanes Rodríguez**,** *"El intrusismo informático como delito autónomo: razones"***,** en Biblioteca jurídica online "elDial.com" (www.eldial.com.ar), suplemento de Derecho Penal y Contravencional de la CABA, sección doctrina, diciembre de 2008.

[10] Sáez Capel-Velciov, en su *"Comentario al art. 153bis"* pub. en AAVV "Código Penal", dirigido por Baigún y Zaffaroni, ed. Hammurabi, Bs.As., Tomo 5, 2008, págs. 733/735.

[11] Su texto: *"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".*

subjetivos distintos del dolo como la intención de obtener datos u otra intención delictiva. También permite que la tipificación se limite a casos de acceso a sistema informático 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. También que se adopta como sanción la pena privativa de libertad, respuesta que el convenio admite pero no exige. Un problema básico de esto es que si en el delito más leve, básico y de aplicación subsidiaria, se usa la modalidad más grave de sanción, en el resto de las conductas no podrá evitarse sin caer en problemas de serios de proporcionalidad y, en realidad, se trata de un comportamiento sobre el que se discute si realmente es necesaria la intervención del derecho penal o bastaría con la del contravencional o sancionador administrativo, apareciendo como más lógicas las penas pecuniarias o de inhabilitación que la prisión.

Pasando a la descripción legislativa en el ámbito del Mercosur, puede señalarse que el "intrusismo informático" sólo no ha sido expresamente tipificado en Brasil, Chile y Uruguay, razón por la que en el detalle que sigue se los dejará para el final. Veamos.

b.1. Bolivia: 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. 363ter[12] de su CP del año 1997.

b.2. Colombia: su C.P. (Ley 599 de 2000) ha sido modificado por la Ley 1273 de 2009, que le incorporó como cap. VII bis uno especifico para la delincuencia informática. El acceso abusivo a un sistema informático está contemplado en el art. 269A[13]. Debe tenerse además presente que todas las conductas del capítulo tienen previstas una serie de circunstancia de agravación en el artículo final, el 269H[14].

[12] 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"*.

[13] 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"*.

[14] 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.

b.3. Ecuador: a continuación del art. 202 CPE, por Ley 2002-67, se agregó n artículo sin número[15] 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.

b.4. Paraguay: conducta típica a partir de la reforma del CP por Ley 4439 del año 2011, prevista en el nuevo art. 174 b[16].

b.5. Perú: incorporó en su Parte Especial por Ley 27309 (17/7/00), en el Título V de los delitos contra el patrimonio, un nuevo capítulo X "Delitos Informáticos", con tres artículos. El primero de ellos (art. 207-A[17]), pune 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) agrava los anteriores en caso de que el acceso su hubiere logrado usando información privilegiada o se pusiere en peligro la seguridad nacional.

b.6. Venezuela: prevé el "acceso indebido" en el art. 6[18] de la "Ley Especial contra los Delitos Informáticos" (LECDI), del año 2001. A su vez, el art. 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 incrementará las penas entre

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".

[15] La parte pertinente dice: *"Art. ... (1).- (Ag. por art. 58, Ley 2002-67, R.O. 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".

[16] 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 inciso 1°, se entenderán solo aquellos, que se almacenan o transmiten electrónicamente, magnéticamente o de otra manera no inmediatamente visible"*

[17] Dice: *"Artículo 207-A.- El que utiliza o ingresa indebidamente a una base de datos, sistema o red de computadoras o cualquier parte de la misma, para diseñar, ejecutar o alterar un esquema u otro similar, o para interferir, interceptar, acceder o copiar información en tránsito o contenida en una base de datos, será reprimido con pena privativa de libertad no mayor de dos años o con prestación de servicios comunitarios de cincuentidós a ciento cuatro jornadas.*
Si el agente actuó con el fin de obtener un beneficio económico, será reprimido con pena privativa de libertad no mayor de tres años o con prestación de servicios comunitarios no menor de ciento cuatro jornadas"

[18] 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 información, será pena con prisión de uno a cinco años y multa de diez a cincuenta unidades tributarias".*

una tercera parte y la mitad. A su vez, el art. 21, referido a la violación de la privacidad de las comunicaciones, entre otras conductas sanciona al que mediante el uso de las tecnologías de la información acceda a 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.

b.7. Brasil: donde la conducta sería atípica con la salvedad de la regulación especial de su Ley Electoral N° 9100 del año 1995, con motivo de la incorporación del sistema de voto electrónico en las elecciones de 1996, por cuyo 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.

b.8. Chile: tampoco lo prevé en forma directa.

b.9. Uruguay: no hay un tipo específico, pero se ha verificado una condena por esta conducta, que se subsumió bajo la figura del art. 300 del C.P.[19], que pena el "conocimiento fraudulento de secretos" que pareciera más apto para los casos de intercepción ilícita.

2. Tipo Objetivo

a) Bien jurídico

No se habrán de reiterar aquí las consideraciones generales brindadas al comentar el art. 153. En particular con relación al tipo que ahora se comenta, apuntan José Sáez Capel y Claudia E. Velciov que se pretende fundar su punibilidad como delito de peligro, entendiendo que el mero instrusismo o acceso informático ilegítimo, en sí mismo importa un nivel de riesgo considerable, además de privar al titular de la información a la que se accede de su confidencialidad y exclusividad, lo que vulnera el ámbito de su intimidad como extensión de los atributos de la persona. En lo específico, afirman, esta figura supone vulnerar la confidencialidad de la información en sus dos aspectos: exclusividad e intimidad[20].

[19] 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)".*

[20] Ob.cit., pág. 740. Ccte.: Marco Antonio Terragni, *"Tratado de Derecho Penal"*, Ed. La Ley, Bs.As., Tomo II "Parte Especial – I", 2012, pág. 541.

Amans y Nager, por su lado, con restricción que no compartimos sostienen que lo protegido es el secreto de los datos resguardados en sistemas informáticos de entes públicos y financieros[21], mientras que Morosi y Viera se limitan a destacar que la figura se ocupa del instrusismo propiamente dicho, despojado de cualquier otra intención distinta del acceso mismo[22].

Sin embargo, nos parece más apropiado para evitar o corregir posibles extensiones inadmisibles del ámbito de lo prohibido en esta figura de cuestionada inclusión en el ámbito penal, que el análisis del bien jurídico afectado no haga foco, exclusivamente, en el acceso mismo, en la información en sí o en la utilidad de los sistemas informáticos y la necesidad de preservarlos. Aunque ello sea merecedor de tutela, luce evidente que esta puede brindarse más eficazmente en el ámbito administrativo, e incluso, contravencional. Preferimos, en cambio, centrar la atención en que la protección penal se haga sin descuidar el contenido mismo que soporta el dato o sistema informático y que, por algún motivo, su titular no lo hace de público conocimiento, restringiendo su acceso en vistas de resguardar su valor confidencial y, con ello, su derecho subjetivo.

De esta forma, no nos alejamos de la protección a la intimidad en la sistemática del código, con consideraciones vinculadas al objeto material o a los medios que, con la distancia tomada, nos acercan a la punibilidad de meras infracciones. Así, en resolución que pareciera atender demandas del principio de lesividad, se ha declarado atípica la conducta de acceder al historial de correos electrónicos de un usuario en la inteligencia que esto no implica acceder a su contenido[23].

Obsérvese también que, podría darse el caso de datos que aunque se hallen en archivos securizados, no son confidenciales, sino de uso o dominio público. Por otra parte, aunque se lo caracterice como un delito de peligro, no excluimos la consideración del resultado –peligro concreto- que acontece de manera instantánea con el acceso ilegítimo en las circunstancias típicas (por ej. una vez descifrados los códigos de acceso).

También nos parece importante aclarar, aunque parezca algo obvio, que el valor confidencial del dato o sistema informático no es igual a su caracterización como personal, si bien ambos atañen a la privacidad. En este sentido, a diferencia de otras legislaciones, el código prevé dos figuras de acceso ilegítimo, indebido o no autorizado a sistemas informáticos y así, junto al acceso a un sistema

[21] Carla V. Amans y Horacio S. Nager, *"Manual de Derecho Penal. Parte Especial"*, dirigido por Carlos A. Elbert, Ad-Hoc, Bs.As., 2009, pág. 211.
[22] Morosi, Guillermo E.H. - Viera, Mariano A.: *"Comentario al art. 153"*, pub. en AAVV *"Código Penal de la Nación, Comentado y Anotado"*, Andrés José D´Alessio director, La Ley, Bs.As, 2da. ed., T. II, 2011, pág. 530.
[23] Así, la Sala I de la CFCyC, en causa N° 42063 "Caballero, F.", resuelta el 6/8/09, cf. individualiza Aboso, ob.cit., pág. 766.

o dato de ingreso restringido que estamos analizando, el Código Penal establece en su art. 157 bis la prohibición de acceso ilegítimo a bancos de datos personales, tipicidad que incluso le precede ya que había sido incorporada en el año 2000.

b) Verbo típico

La conducta típica consiste en el acceder sin autorización o excediendo la que se tiene a un sistema o dato informático de acceso restringido. Con esta última precisión ("acceso restringido"), contenida al cierre del primer párrafo, se excluye la posibilidad de punir el acceso a redes, sistemas y contenidos de sitios públicos. La restricción podrá ser mediante una clave –de usuario- o cualquier otra modalidad limitativa que exprese que se trata de ámbito reservado por el titular –contraseña o password-.

Aboso, siguiendo criterio de la Sala II de la CFCyC, incluye el acceso a dato "restringido" incluido en un sistema informático de acceso público[24], como podrían ser datos sensibles de usuarios que se pudieran almacenar en dicho sistema. Terragni, por su lado, habla de la posibilidad de que el acceso sea total o parcial al sistema[25].

c) Otros elementos del tipo objetivo

En cuanto a las definiciones de las expresiones "sistema informático" y de "dato informático", el art. 1 del *"Convenio sobre Cibercriminalidad"* de Budapest (2001), en sus incs. "a" y "b", nos provee las siguientes: *"A los efectos del presente Convenio, la expresión: a. "sistema informático" designa todo dispositivo aislado o conjunto de dispositivos interconectados o unidos, que aseguran, en ejecución de un programa, el tratamiento automatizado de datos; b. "datos informáticos" designa toda representación de hechos, informaciones o conceptos expresados bajo una forma que se preste a tratamiento informático, incluido un programa destinado a hacer que un sistema informático ejecute una función;…"*.

A su vez, en nuestro derecho interno, la Ley 25326 de Protección de Datos Personales (2000), en su art. 2 "Definiciones", nos dice que "datos informatizados" son *"Los datos personales sometidos al tratamiento o procesamiento electrónico o automatizado"* y, a su vez, que los "datos

[24]Aboso hace referencia a la causa N° 28260 "Incidente de incompetencia por violación de correspondencia", resuelta el 8/9/09 (en su *"Código Penal de la República Argentina. Comentado, concordado con jurisprudencia"*, Ed. BdeF, Bs.As., 2012, pág. 766).
[25] Ob.cit., pág. 542.

personales" son la *"Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables"*, mientras que "datos sensibles" son los *"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"*, debiéndose entender por "tratamiento de datos" 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"*.

d) Casos de atipicidad:

Así como vimos en el tipo anterior excepciones al principio de la inviolabilidad de las comunicaciones, que implicaban que el derecho protegido no era absoluto (autorizaciones judiciales para su acceso en curso de una investigación penal, o por razones de seguridad, o por cumplimiento efectivo del ejercicio de un deber derivado de la patria potestad, etc.), lo propio ocurre aquí, por lo que interesa determinar cuándo terceras personas que no son los legítimos usuarios de los datos y sistemas informáticos comprometidos, pueden acceder a ellos aunque, claro está, no estén debidamente autorizados de antemano.

d.1. *Por consentimiento del usuario*: naturalmente que la prohibición queda excluida desde el punto de vista del análisis conglobado del tipo cuando la acción de acceder a datos o sistemas informáticos de ingreso restringido, se realiza de manera coetánea con el consentimiento del sujeto pasivo[26]. Pero, en la medida en que la falta de autorización debida es un elemento normativo del tipo, el acuerdo previo con terceros legitima el accionar y directamente elimina el tipo objetivo sistemático.

La autorización puede ser formulada de cualquier forma aunque, por lo general, cuando se trata de un permiso previo, se entiende traducida en un contrato de prestación de servicios de seguridad informática[27].

[26] Ccte.: Buompadre, *"Tratado de derecho penal. Parte especial"*, Astrea, Bs.As., 3° edición actualizada y ampliada, 2009, pág. 713.
[27] Sáez Capel y Velciov, ob.cit., pág. 744.

d.2. *Por seguridad:* es otras de las razones por las que se analiza el recorte al tipo legal, con el objetivo de facilitar a los ingenieros de sistemas o expertos en programación de software y seguridad informática su trabajo específico, por ejemplo, para determinar las falencias de las redes informáticas, la identificación de posibles virus, el testeo de sistemas de bloqueo, etc.

El tipo no distingue la forma de intrusismo, de modo que el acceso bien puede realizarse mediante la utilización de los datos concernientes al sujeto pasivo, es decir, como si el autor fuera en realidad el legítimo usuario del sistema, o aprovechando las deficiencias de los procedimientos de seguridad del sistema o en alguno de sus procedimientos[28], o usar un programa desencriptador.

Esto último es importante porque, por lo general, implica una razón de uso que permite excluir del tipo los casos de los programadores o "hackers éticos", que acceden mediante el hecho de poder abrir claves o puertos en una computadora o red informática, con herramientas de software dedicadas a tal fin para el testeo y con el objetivo de resguardar, reestablecer o mejorar el sistema. Coincide con esta perspectiva Palazzi cuando destaca que quedan fuera del ámbito típico las conductas de testeo de seguridad de falencias de redes informáticas ("ethical hacking") en el marco de investigación académica, casera o empresaria, muchas veces realizado además con consentimiento de la "víctima", interesada en la detección de errores para su subsanación[29].

Ciertamente que, en la práctica, frente a la alternativa de posible daño, sabotaje o pérdida de información (hacking indirecto o como medio de comisión de otros delitos), la intromisión ocurre, por lo general, con el consentimiento del dueño o titular de la red que está siendo testeada, por lo que existe un autorización por parte del damnificado. De cualquier manera, si ello no fuera tan claro, sino dudoso o discutido, podría el operador quedar amparado por una situación de necesidad, sacrificándose la confidencialidad hacia él en pos de evitar directamente la pérdida de la información confidencial, es decir, con el bien u objetivo mayor de resguardar el sistema que tiene por fin, precisamente, preservar la información de carácter reservado. De modo que, posiblemente, el ámbito mayor de discusión, esté dado en términos de exceso de autorización o de justificación.

También señala Palazzi como fuera del ámbito típico la denominada ingeniería inversa o reversa, que es la destinada a obtener información técnica a partir de un producto accesible al público (como programas de computación y componentes electrónicos), con el fin de determinar de qué está hecho, qué lo hace funcionar y cómo fue fabricado, actividad que evidentemente no se relaciona con

[28] Cf. Morosi-Viera, ob.cit., pág. 531.
[29] En *"Análisis de la ley 26388 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, pág. 1217.

la "privacidad" sino, a todo evento, con la protección de la propiedad intelectual (ámbito en el que se encuentran reguladas sus limitaciones, recordando el nombrado que nuestro país, pese a haber aprobado el "Tratado de Derecho de Autor de la OMPI del año 1996", no lo ha reglamentado aún ni en lo civil ni en lo penal, por lo que bien podría incluirse este tema en el siguiente acápite, destinado a aquellos problemas que no tienen clara solución)[30].

A efectos de evitar cualquier interpretación incorrecta de lo afirmado, quede claro que cuando aludimos al interés académico no nos estamos refiriendo a las consignas ─que Durrieu y Lo Prete califican de "escandalosas"─ del tipo "sólo con fines educativos" que usan algunas páginas webs dedicadas a "instruir" y proporcionar medios para "hackear". No se trata de habilitar la posibilidad de "educar para el delito"[31].

d.3. *Por cumplimiento del deber*: otro caso de atipicidad estaría dado por el cumplimiento de un deber derivado de un mandato judicial fundado en el marco de una investigación, por ejemplo, que autorice el acceso a la información que pueden brindar los programas digitales de telefonía celular, generalmente utilizados a nivel comercial para facturación, con el objetivo de ubicar a una determinada persona, independientemente de la comunicación que entable, su itinerario en virtud de la información de antena, la activación de GPS, etc.

e) Sujeto activo

[30] Idem. anterior. De cualquier manera, vale aclarar que los componentes más comunes que son sometidos a la ingeniería inversa son los programas de computadora y componentes electrónicos. Esto facilita la sustracción ilegítima de teléfonos celulares ante la facilidad de abrirlo y poder hacerlo funcionar con otro proveedor distinto, de modo que, debería regularse la forma en que las empresas de servicios impidan la instalación de "chips" en aparatos sustraídos.

[31] Durrieu, Roberto y Lo Prete, Justo, en su artículo *"Delitos Informáticos"*, pub. en L.L., diario del 1/2/02, pág. 2. Palmario ejemplo de este orden de problemas es el recordatorio de Nehemias Gueiros Jr., cuando informa de casos como el del famoso programa creado por el grupo de hackers "Cult of the Dead Cow" (Culto de la vaca muerta) llamado "Back Orifice" (entrada o puerta trasera), para espiar en forma remota las claves tecleadas en una máquina, que está disponible gratuitamente en Internet, así como otras herramientas similares como el "Sub-seven". Sitios que auxilian a planear ataques a otros computadores como hack.co.za o astalavista.box.sk, hacen realidad la idea de que cualquiera que sepa teclear es capaz de producir alguno de estos comportamientos ilícitos, lo que lleva a concluir al autor citado que esto prueba que Internet es realmente incontrolable (en su artículo *"Insegurança na Internet: há remédio?"*, pub. en el portal jurídico "Mundo Jurídico" –www.mundojuridico.adv.br─, en 30/7/03.

El sujeto activo o intruso, puede ser cualquiera, aunque, por tratarse de un delito vinculado a las nuevas tecnologías de la información requiere, naturalmente, ciertos conocimientos mínimos para que, bajo el criterio de la dominabilidad, pueda serle imputable el tipo objetivo como obra propia.

Se trataría de a quien en la jerga se denomina "hacker", derivado del vocablo inglés "hack" cuya traducción literal sería "cortador" o "hachador" que, conforme recuerda Jorge Rudi, se comenzó a utilizar a comienzos de los ochentas en Estados Unidos para designar a quien intercepta en forma dolosa un sistema informático para apoderarse, interferir, dañar, destruir, difundir o hacer uso de la información que se encuentre almacenada en los ordenadores pertenecientes a entidades Públicas, Privadas, Fuerzas Armadas o de Seguridad, Entidades Financieras y usuarios particulares[32]. Hoy día con el término se alude a alguien con amplios conocimientos del lenguaje de programación que le permiten detectar fallas o "agujeros" para acceder al sistema[33]. Sin embargo, es fácil advertir que una persona que puede ser un simple operador o usuario[34], con un saber técnico muy limitado, puede llevar adelante la conducta típica por haber conocido la clave por un descuido de su titular.

Entendemos que, aunque ocasionalmente pueda seguirse mencionando, estamos ya lejos de aquellas caracterizaciones que se formulaban a comienzos de los noventa, cuando Sieber al hablarnos de los potenciales autores de delitos informáticos mencionaba que en ellos campeaba una "a*ctitud o espíritu deportivo"*, que se trataba de personas brillantes, sobre todo jóvenes, que sienten el desafío y satisfacen su ego venciendo los controles que les interpongan. En ese contexto, resaltaba que los accesos no autorizados a los sistemas de proceso de datos se cometen, en primer lugar, por piratas juveniles, que actúan por diversos motivos (alardear, divertirse, vencer el reto, etc.), pudiéndose hablar por analogía de "delincuencia de pantalones cortos" (*short-pants crime*). Una actividad característica de este móvil sería el "hacking", al que el autor mencionado definía como el *"acceso no autorizado a un sistema de proceso de datos a través de un proceso de datos a distancia, no cometido con finalidades manipulatorias, fraudulentas, de espionaje, ni de sabotaje, sino sencillamente como paseo por placer no autorizado (joyriding) por el ordenador de otra empresa*

[32] Cf. Rudi, *"Las actas de 1984 y 1986 sobre delitos informáticos en los Estados Unidos de América"*, pub. en E.D., T. 159 (1994-2), págs. 1055/1061, donde noticia que en U.S.A. la actividad del hacker comenzó a penalizarse específicamente en la *"The counterfait acces device and computer fraud and abuse act of 1984"* que, agregamos, ha recibido desde entonces numerosas y sucesivas sustituciones.
[33] Así, Morosi-Viera, ya citados, pág. 531.
[34] Cf. el art. 2 de la Ley 25326, "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 los mismos"*.

("hackito ergo sum")", pudiendo ser catalogado como una forma especial de 'hurto de servicios'..."[35].

Más aún, desde el estudio del punto de vista criminológico, se ha referido una especie de subcultura del hacker o pasión por el intrusismo informático (hackerdown)[36] compuesta por personas particularmente creadoras, ingeniosas, que incluso comparten un vocabulario especial como herramienta de comunicación, dedicados y apegados a la tecnología para explorarla, analizarla, modificar su funcionamiento y compartir la información restringida que brinda.

Cuando se incluye a quien teniendo autorización la excede, podría tratarse de aquellos que Aboso llama "confidentes necesarios", que son aquellas personas que tienen a su cargo el procesamiento de datos o quienes están encargados de la supervisión general del funcionamiento del sistema que acceden a bases de datos restringidos[37].

f) Sujeto pasivo

El sujeto pasivo será el titular del sistema o dato informático. Que este sea un organismo público o un proveedor de servicios públicos o financieros, opera como calificante del tipo.

Conforme el art. 2 de la LPDP (N° 25326, del año 2000), el "titular de los datos" es *"Toda persona física o persona de existencia ideal con domicilio legal o delegaciones o sucursales en el país, cuyos datos sean objeto del tratamiento al que se refiere la presente ley"*.

3. Tipo Subjetivo

[35] Ulrich Sieber, en su trabajo *"Criminalidad Informática: Peligro y Prevención"*, pub. en AAVV *"Delincuencia Informática"*, Santiago Mir Puig compilador, Edit. PPU, Barcelona, 1992, págs. 13/45. Similar padecimiento de falta de actualidad padecen otras clasificaciones como aquella que diferencia del hacker al "phreaker" (contracción de *freak, phone y free,* "adicto a los estupefacientes", "teléfono" y "gratuito", respectivamente, podría traducirse como *adicto a las comunicaciones gratuitas*); al "virucker" (apócope de *virus y hacker*, variante del hacking que también se ha denominado "cyberpunks"); al "pirata informático" (dedicado a afectar la propiedad intelectual) o al "propagandista informático", rubro donde podría ubicarse la actividad de *"detentación y difusión abusiva de códigos de acceso"* (sobre esto nos extendimos en Riquert, *"Informática y derecho penal argentino"*, Ad-Hoc, Bs.As., 1999, cap. IV "Observaciones criminológicas").

[36] Saéz Capel, J. "Informática y delito", Proa XXI Ed., Bs.As., 1999, p.89/92.

[37] Cf. el art. 2 de la Ley 25326, el "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"*.

Aquí se trata de la voluntad de intromisión o ingreso al sistema de tratamiento de información o dato informático restringido, con el conocimiento que el acto es ilegítimo, es decir, que se carece de derecho, permiso, autorización o consentimiento para hacerlo.

El primer párrafo, que consagra la punición como conducta básica de quien con conocimiento y sin autorización o excediéndola, accede por cualquier medio a un sistema o dato informático de acceso restringido, deja fuera por medio de este requerimiento cognitivo (*"a sabiendas"*), la punición de todo acceso fortuito, casual o imprudente. Se trata de un tipo doloso, que por este condicionamiento subjetivo es sólo compatible con el dolo directo, excluyendo al eventual[38].

El tipo no requiere elementos subjetivos distintos del dolo, esto es, de tendencia interna trascendente (ultrafinalidades usualmente destacadas con la preposición "para" o "con el fin de") o peculiar o con cierto ánimo. Por ello, cualquier otra finalidad que la descripta sería propia de algún delito más grave y por esta razón se ha caracterizado al sujeto activo como el autor que procura eliminar los pasos de seguridad del sistema para ver el contenido de la información protegida[39].

El error sobre un elemento del tipo objetivo excluye el dolo y la responsabilidad penal tanto si es invencible como vencible, dado que no se encuentra previsto el tipo culposo.

Una mención especial efectúa Rueda Martín en torno al *"error in personam"*, supuesto en que el autor accede a datos de una persona distinta de la que el se había representado, por haberla confundido con ésta. Siendo que el bien jurídico en este tipo es de carácter personalísimo, el sujeto pasivo que debería ser aquella persona titular de los datos, no es equivalente desde el punto de vista de la protección penal y aunque el elemento subjetivo del injusto concurre, la acción no se dirigía a causar el perjuicio de esa persona en concreto sino de otra diferente, por lo que , aprecia en estos casos una tentativa de delito[40].

4. Iter críminis

[38] Cctes.: Sáez Capel y Velciov, ob.cit., pág. 746.
[39] Ccte.: D´Alessio, ob.cit. pág.532.
[40] María Ángeles Rueda Martín, "La Protección Penal de la Intimidad Personal e Informática", Ed. Atelier, Justicia Penal, Barcelona, 2004, pág. 85.

El delito se consuma en el momento en que se concreta el acceso al sistema o al dato informático restringido, o para quien está autorizado a acceder, en el momento en que se excede el límite de tal autorización.

Se lo ha caracterizado como delito "de antesala" o "delito barrera o obstáculo"[41] en virtud de que se trata de una figura que opera subsidiariamente, cuando no se puede acreditar la realización de otra más grave como la alteración o supresión de datos. Sin embargo, corresponde tener presente que, por lo general, los hackers evitan que su acceso ilegítimo sea descubierto y, por lo tanto, no destruyen datos ni dañan o alteran el sistema, en procura de que su presencia no llame la atención del administrador o usuario del caso[42].

También se lo presenta como un tipo de pura actividad y de peligro[43], advirtiendo incluso que incorrectamente interpretado podría constituirse en una suerte de acto preparatorio punible con olvido del principio de lesividad[44].

La tentativa es posible: basta pensar en los casos de uso de programas que operan por "fuerza bruta", es decir, introduciendo sucesivamente todas las posibles alternativas de combinación alfanuméricas que constituyen una clave, supuestos en los que podría interrumpirse el "iter" entre el comienzo de ejecución y la consumación[45].

Precisamente, cuando aún no estaba tipificada la conducta, uno de los primeros casos que en nuestro país generó discusión alrededor de la conducta de mero intrusismo involucró el servidor de la U.N. de Río Cuarto y se trató de un acceso no autorizado que quedó en grado de tentativa (fallo del 26/4/99, causa *"Universidad Nacional de Río Cuarto s/denuncia"*, Secretaría del Dr. Carlos A. Ochoa). El Juez Federal de Río Cuarto, Dr. Luis R. Martínez, concluyó en aquel momento que la conducta consistente en intentar ingresar a un servidor no disponible al público sino a través del conocimiento de una clave, mediante la utilización de Internet no constituía delito, por lo que desestimó la denuncia y ordenó su archivo[46].

5. Concursalidad

[41] Cctes.: Sáez Capel y Velciov, ob.cit., pág. 747.
[42] Sáez Capel y Velciov, ya citados, pág. 747.
[43] Así, Morosi-Viera, ya citados, pág. 532.
[44] Cf. Amans-Nager, ya citados, pág. 215.
[45] En contra: Buompadre, ob.cit., pág. 714, inc. f), donde luego de caracterizar la figura como delito de pura actividad y de peligro abstracto, manifiesta que la tentativa no le parece posible.
[46] Pub. en J.A., revista 6157 del 1/9/99, pág. 22.

Al indicar *"si no resultare un delito más severamente penado"* fija con claridad el carácter subsidiario, residual o remanente asignado a la figura, lógico si se atiende a que como ya se ha enfatizado, en general, en el derecho comparado, se ha entendido que estamos frente a una conducta de "antesala" cuya punición ha sido producto de gran discusión.

La posibilidad de concurso con el art. 153 ha sido afirmada por la Sala VII de la CNCyC diciendo: *"Si se tuvo por acreditado que el damnificado no pudo ingresar a su casilla de correo electrónico a raíz de que el imputado habría cambiado su clave de acceso y que ello motivó la difusión de información privada y laboral al día siguiente en la institución en que aquel se desempeñaba, que sólo pudo filtrarse con la exclusiva lectura directa de la casilla, es válido sostener que tal comportamiento se adecuaría a las figuras previstas en los artículos 153 y 153bis del Código Penal. Por tanto, corresponde revocar el sobreseimiento apelado"*[47].

Aún reconociendo las limitaciones para sacar conclusiones que impone lo que no es más que un extracto, parece difícil admitir que el relatado sea un supuesto de concurso de delitos. Buompadre destaca que, conforme la regla de subsidiariedad, el desplazamiento se producirá cuando el hecho mismo del ingreso al sistema informático pasa a configurar otro delito más severamente penado, lo que sucede cuando el acceso es un elemento que integra la tipicidad de la acción de otro delito o cuando en sí mismo el hecho constituye el corpus del delito más grave[48]. Aplicado al supuesto de hecho expuesto, sería la figura del art. 153 la que por relación de especialidad desplazaría la de simple intrusismo.

Por último, puede mencionarse la posibilidad de quedar vigente el tipo en comentario en caso de mediar un desistimiento de figura más grave como, por ejemplo, daño o sabotaje informático o una estafa informática (CP, arts. 183 y 173 inc. 16, respectivamente).

6. Pena. Agravante.

El segundo párrafo duplica la pena cuando el acceso fuere respecto de un sistema o dato informático de un organismo público estatal o un proveedor de servicios públicos o de servicios financieros. La distinción aparece razonable y, en consecuencia, importa la calificación de la figura

[47] Causa "M.,M.", fallo del 21/10/10, extractado por Mariana Salduna en la obra de Edgardo A. Donna y otros, *"El Código Penal y su interpretación en la jurisprudencia"*, Rubinzal-Culzoni editores, Santa Fe, 2° edición ampliada y actualizada, 2012, Tomo III "Arts. 118 a 171", págs. 359/360.
[48] Ob.cit., pág. 713.

por la característica singular del sujeto pasivo. En cuanto al concepto de "servicio público", con cita a Durrieu y Lo Prete, los ya mencionados Sáez Capel y Velciov lo definen como *"todo aquel que se encuentre destinado a servir a la población en forma más o menos generalizada, a un número de personas indeterminado, más allá de que su prestación corra por cuenta del Estado o de particulares"*[49].

Entendemos que habiéndose optado por la criminalización de esta conducta disvaliosa resignando la vía contravencional, que preferíamos[50], al menos podría haberse evitado la utilización de la pena privativa de libertad en la figura básica. Es claro que no sólo en el imaginario colectivo, sino en la mente del legislador, sigue instalada férreamente la idea de que "penar" significa "privar de libertad". No albergo dudas de que estamos frente a una conducta que tendría una respuesta punitiva más racional si se la hubiese conminado con multa o alguna inhabilitación especial o alternativa reparatoria.

Es más, en el Anteproyecto de ley que había elaborado la Secretaría de Comunicaciones de la Nación[51], abierto en su oportunidad a discusión pública, se preveía una figura similar en el art. 1°[52], para la que conminaba con pena en abstracto de multa de mil quinientos a treinta mil pesos. Comentándola, Arocena expone un criterio similar al antes expuesto, diciendo que *"Se considera apropiada la fijación de una* ***pena de multa,*** *atento que se trata de una figura básica que generalmente opera como antesala de conductas más graves, por lo que no amerita pena privativa de libertad, la que por la naturaleza del injusto habría de ser de muy corta duración"*[53].

7. Acción penal privada

Un paliativo mínimo a una intervención penal que en muchas ocasiones se demostrará innecesaria resulta ser que no se trata de un delito de acción pública, sino privada conforme el inc. 2°

[49] Ob.cit., pág. 747.
[50] Cctes.: Sáez Capel y Velciov, ya citados, pág. 743, donde manifiestan que enrolados *"en la corriente mayoritaria sostenemos 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"*.
[51] Pub. en el B.O. N° 29782 del 26/11/01, además del sitio web oficial de la Secretaría.
[52] Su primer párrafo decía: *"Será reprimido con pena de multa de mil quinientos a treinta mil pesos, si no resultare un delito más severamente penado, el que ilegítimamente y a sabiendas accediere, por cualquier medio, a un sistema o dato informático de carácter privado o público de acceso restringido"*.
[53] Gustavo A. Arocena, *"Acerca del principio de legalidad penal y de hackers, crackers, defraudadores informáticos y otras rarezas"*, pub. en portal jurídico del Centro de Investigación Interdisciplinaria en Derecho Penal Económico (www.ciidpe.com.ar), sección temática 2, "Derecho Penal Económico. Parte Especial". La cita corresponde al punto V.6.1., dedicado al "Acceso ilegítimo informático".

del art. 73 del CP, que incluye los supuestos de violación de secretos con sola excepción de los arts. 154 y 157.