Fecha de recepción: 31 de enero de 2013 / Fecha de aprobación: 12 de mayo de 2013

Revista de Derecho Comunicaciones y Nuevas Tecnologías

El delito de acceso abusivo a sistema informático: a propósito del art. 269A del CP de 2000

Ricardo Posada Maya

Universidad de los Andes
Facultad de Derecho
Revista de Derecho, Comunicaciones y Nuevas Tecnologías
N.º 9, Junio de 2013. ISSN 1909-7786

El delito de acceso abusivo a sistema informático: a propósito del art. 269A del CP de 2000

Ricardo Posada Maya*

Resumen

El Código Penal colombiano prevé en el artículo 269A el delito de acceso abusivo a sistema informático que, además de proteger directamente la seguridad e integridad de los sistemas informáticos e indirectamente los datos y la información informatizada, como bien jurídico colectivo, también resguarda el derecho constitucional fundamental a la intimidad personal informática (CN, art. 15). Así las cosas, la presente contribución académica realiza un análisis breve de esta importante figura criminal, estudia los bienes jurídicos protegidos por la norma citada y precisa los elementos objetivos y subjetivos que la estructuran en el CP vigente.

Palabras clave: acceso abusivo, sistemas informáticos, medidas de seguridad informáticas, intimidad personal informática, delitos contra la seguridad de los sistemas informáticos, los datos y la información.

Abstract

The Colombian Penal Code provides in article 269A the crime of abusive access to a computer system that, in addition to directly protect the computer system's security and integrity, and indirectly the data and computerized information, as collective interest, also protects the fundamental constitutional right to computer privacy (CN, art. 15). So, this academic contribution make a brief analysis of this important criminal figure, study the legal interest protected by the cited standard and the objective and subjective elements which structure this legal figure in the current criminal code.

Keywords: Abusive access, computer systems, computer security measures, computer privacy, crimes against the security of the computer systems, data and information.

* Profesor asociado del Área de Derecho Penal, Procesal Penal y Criminología, y director del Grupo de Investigación y Estudios en Derecho Penal "*Cesare Beccaria*" de la Universidad de los Andes, Bogotá, Colombia. Conjuez de la Sala Penal de la Corte Suprema de Justicia de Colombia. Doctor y DEA en Derecho por la Universidad de Salamanca (España) y especialista en Derecho Penal por la Universidad de Antioquia.

Sumario

I. CONSIDERACIONES GENERALES

El 5 de enero de 2009 el Gobierno Nacional sancionó la L. núm. 1273[1], mediante la cual fue adicionado un nuevo título VII *bis* al Código Penal (en adelante CP) de 2000 (L. 599 de 2000), denominado *De la protección de la información y de los datos* informáticos. La reforma al CP siguió parcialmente los estándares técnico-dogmáticos sugeridos por el *Convenio de Budapest* del Consejo de Europa (2003) contra la cibercriminalidad (Tít. I, art. 2°)[2].

Una de las figuras ampliamente modificadas por esta ley fue el delito de *acceso abusivo a sistema informático*[3]. Tipo penal pionero en nuestro medio jurídico que inicialmente fue regulado por el art. 195 del CP[4] —dentro del capítulo VII, título III, dirigido a castigar *La violación de la intimidad, reserva e interceptación de comunicaciones*—, y que en esta oportunidad fue incluido en el art. 269A, dentro de las figuras que castigan especialmente "*Los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos"* que los contienen, procesan o transmiten en forma automática. Con ello el legislador penal colombiano confirmó su deseo de garantizar la seguridad de las funciones informáticas propiamente dichas, en contra de ataques cibercriminales[5], como figuras autónomas frente a los tipos penales tradicionales.

Sin embargo, la evolución del mencionado art. 269A no ha sido pacífica. En efecto, el cinco de marzo de 2009, esto es, dos meses después de entrar en vigencia la "ciber-reforma", el Gobierno Nacional sancionó la L. 1288[6] —*mediante la cual se expidieron normas para fortalecer el marco legal que permite garantizar la reserva de la información derivada de acciones de "inteligencia y contrainteligencia"*— que, con evidente falta de planeación legislativa, revivió y modificó, en el art. 25, el invalidado art. 195 CP[7] y derogó los arts. 4° y 269A adicionados por la reciente L. 1273 de 2009.

Para completar el diagnóstico, debe decirse que la L. 1288 de 2009 fue declarada inexequible

1 Ley publicada en el *Diario Oficial* núm. 47.223 del 5 de enero de 2009.

2 Precisamente, la "*Convention on Cybercrimen*" (ETS. núm. 185/2003), consultada en lengua inglesa, en: http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm.

3 L. 1273 de 2009, art. 4°: "La presente ley rige a partir de su promulgación y deroga todas las disposiciones que le sean contrarias, en especial el texto del artículo 195 del Código Penal". La ley hizo en este caso una derogatoria especial.

4 El CP, art. 195 decía así: "El que abusivamente se introduzca en un sistema informático protegido con medida de seguridad o se mantenga contra la voluntad de quien tiene derecho a excluirlo, incurrirá en multa". Respecto a los delitos informáticos contemplados antes de la reforma, y en particular sobre el acceso abusivo a sistema informático protegido con medida de seguridad, v. Posada Maya (2006b, pp. 23 y ss.) y Castro Ospina (2001).

5 Este objetivo fue ampliamente ratificado en: República de Colombia, Departamento Nacional de Planeación, Consejo Nacional de Política Económica y Social. Documento Conpes No. 3701: "Lineamientos de política para Ciberseguridad y Ciberdefensa", Versión Aprobada (14 de julio), Bogotá, Ministerio del Interior y de Justicia (y otros), 2011. Consultado en: https://www.dnp.gov.co/LinkClick.aspx?fileticket=-lf5n8mSOuM%3D&tabid=1260

6 Ley publicada en el *Diario Oficial* núm. 47.282 del 05.03.2009. La modificación más importante de la norma original consistió en eliminar la exigencia de que el sistema informático estuviera protegido con una medida de seguridad informática. También se modificó la punibilidad, esto es, se derogó la pena de multa progresiva en modalidad de unidad multa y se instauró la pena de prisión.

7 L. 1288 de 2009, art 195. Acceso abusivo a un sistema informático. "El que abusivamente se introduzca en un sistema informático protegido con medida de seguridad o se mantenga contra la voluntad de quien tiene derecho a excluirlo, incurrirá en pena de prisión de cinco (5) a ocho (8) años".

por la Corte Constitucional mediante sentencia C-913 de 2010, debido a evidentes vicios de procedimiento en su formación (reserva de ley estatutaria), que de nuevo dejaron vigentes los arts. 4° y 269A de la "ciberreforma".

No obstante, el asunto no terminó allí, porque el Gobierno Nacional presentó de nuevo el Proyecto de ley estatutaria num. 263 de 2011 Senado y 195 de 2011 Cámara de Representantes, "Por medio de la cual se expiden normas para fortalecer el marco jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contra inteligencia cumplir con su misión constitucional y legal, y se dictan otras disposiciones", que fue sancionado como la L. 1621 de 2013. Justamente, dentro de las otras disposiciones, se incorporó un art. 40 en el que se propuso una antitécnica modificación al CP, art. 269A, del siguiente tenor literal:

> Art. 269A. Acceso abusivo a un sistema informático. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el derecho legítimo a excluirlo, incurrirá en pena de prisión de cinco (5) a ocho (8) años y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes. / La pena se aumentará el doble cuando el acceso abusivo beneficie a miembros de grupos armados al margen de la ley u organizaciones de crimen organizado, o cuando el acceso abusivo beneficie a gobiernos extranjeros.

Una reforma muy cuestionable a dos aspectos de la norma vigente. En primer lugar, porque solo buscaba incrementar las penas hasta un máximo imponible de diez (10) años de prisión, cuando el estándar internacional señala como un máximo de pena proporcional y razonable cinco (5) años. Se trata de una tendencia usual en nuestro medio asociada al maximalismo punitivo y al terror penal o neopunitivismo. Y en segundo lugar, por la inclusión de una agravante típica que, si bien era muy interesante en términos político-criminales al recoger parcialmente la figura del ciberespionaje (acceso a los sistemas que almacenan datos de inteligencia y contra inteligencia), fue construida a partir de un resultado de peligro, absolutamente gaseoso (*beneficie*), que sin duda constituye una cláusula general que vulneraba el principio de legalidad.

Dicha propuesta legislativa, para mayor vergüenza del Congreso, también fue declarada inexequible por la Corte Constitucional en la sentencia C-540 de 2012, de nuevo por vicios de forma, al quebrantar el art. 158 superior (CN), que regula el principio de unidad o relación de materia de las leyes o conexidad sustancial[8]. Lo que mantiene incólume la vigencia actual del CP, art. 269A.

La difícil vigencia de esta figura delictiva demuestra la compleja y enorme improvisación le-

8 Dicha sentencia afirma: "Las reformas que se buscan introducir a las disposiciones penales tienen como propósito común hacer más drásticas las penas, además de establecerse circunstancias de agravación punitiva, solo en materia de inteligencia y contrainteligencia. No obstante, en la forma como se procedió por el legislador, terminó por desconocer el principio de unidad de materia, al cumplirse sobre disposiciones penales que, según se ha señalado, comprometen asuntos de contenido diverso y ámbitos de regulación distintos, por lo que resulta imposible establecer una relación de conexidad causal, teleológica, temática o sistémica con la materia dominante del proyecto de ley, como lo es la garantía a la reserva legal de la información de inteligencia y contrainteligencia. De este modo, al no encajar dentro del título que delimita la materia objeto de legislación, se desconoce el principio de unidad de materia".

gislativa que ha rodeado la regulación de estas modalidades criminales en Colombia, que buscan prevenir riesgos masivos y continuos que puedan afectar el funcionamiento confiable y el uso debido de los sistemas informáticos. Sobre este asunto se ha dicho en otra oportunidad que:

> La cibercriminalidad cubre aquellas conductas punibles realizadas con fines ilícitos, no consentidas (facultadas) por el titular de la información o los datos, o abusivas de este consentimiento (facultad), que se orientan a la indebida creación, procesamiento, almacenamiento, adquisición, transmisión, divulgación, daño, falsificación, interceptación, manipulación y ejecución automática de programas de datos o información informatizada reservada o secreta de naturaleza personal (privada o semiprivada), empresarial, comercial o pública, que pongan en peligro o lesionen (CP/art. 11) la seguridad de las funciones informáticas en sentido estricto, esto es, la confiabilidad (calidad, pureza, idoneidad y corrección), la integridad y la disponibilidad de datos o información, y de los componentes lógicos de la programación de los equipos informáticos o de los programas operativos o aplicativos (software). Por consiguiente, no se trata de delitos comunes sino de tipologías especiales realizadas a través de procedimientos informáticos, que gozan de cierta riqueza técnica, aunque no abandonan los tipos penales ordinarios como referentes dogmáticos y criminológicos. (Posada Maya, 2012b, p. 6)[9].

Así las cosas, el presente escrito examina la figura típica informática de *acceso abusivo a sistema informático*. Para ello, en primer lugar, se realizan algunas consideraciones generales. En segundo lugar se estudia la norma prevista en el CP, art. 269A, y se analizan sus elementos dogmáticos objetivos y subjetivos. Finalmente, en tercer lugar, se realizan algunas consideraciones a título de conclusión. Todo ello con el propósito de esclarecer esta compleja figura jurídica que, en la práctica, se advierte como el punto inicial de los cibercrímenes previstos en la legislación vigente[10-11].

II. ASPECTOS DOGMÁTICOS DEL TIPO DE ACCESO ABUSIVO A SISTEMA INFORMÁTICO PROTEGIDO CON MEDIDA DE SEGURIDAD

El legislador penal reguló en el CP, art. 269A adc. L. 1273 de 2009, el tipo penal de *Acceso abusivo a sistema informático*, de la siguiente forma:

9 V. Posada Maya (2006b, pp. 18 y ss.). Romeo Casabona (2006, p. 11) señala que: "Por cibercrimen podemos entender el conjunto de conductas relativas al acceso, apropiación, intercambio y puesta a disposición de información en redes telemáticas, las cuales constituyen su entorno comisivo, perpetradas sin el consentimiento o autorización exigibles o utilizando información de contenido ilícito, pudiendo afectar a bienes jurídicos diversos de naturaleza individual o supraindividual".

10 Según el *Informe de ataques contra sistemas informáticos comparado 2011-2012*, identificado: OFPLA-DIPON-109, consultado en: www.policia.gov.co, del 17 de octubre de 2012, la Policía Nacional reportó que en Colombia, durante este período, fueron presentadas 1985 denuncias penales por cibercrímenes, de los cuales 1191 fueron realizados utilizando la Internet; siendo las ciudades más afectadas: Bogotá, Cali y Barranquilla. Los delitos más cometidos fueron los hurtos por medios informáticos y semejantes, y el acceso abusivo a sistemas informáticos (delitos propiamente informáticos). Las tendencias del informe también señalan que, de las 1985 denuncias, 311 fueron accesos abusivos a sistemas informáticos, y produjeron 26 capturas.

11 INPEC (Instituto Nacional Penitenciario y Carcelario), 28 de febrero de 2013, *Informe de "Población de internos por delito"*. Consolidado nacional generado el 04/03/2013 14:03. Documento del Ministerio de Justicia de Colombia. A esa fecha había un total de 6 condenados y 15 sindicados detenidos en cárceles y prisiones nacionales, por el delito de acceso abusivo a sistema informático. Consultado en: http://www.inpec.gov.co/portal/page/portal/INPEC_CONTENIDO/NOTICIAS%20Y%20NORMATIVIDAD/ESTADISTICA/10%20MODALIDADES%20DELICTIVAS%20POBLACI%D3N%20DE%20INTERNOS%20FEBRERO.pdf

> 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 derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes[12].

Se trata de una modalidad típica de *intrusión*[13] que consiste en:

> [...] arrogarse ilegalmente —de forma no autorizada— el derecho o la jurisdicción de intrusarse o 'ingresar' en un sistema informático o red de comunicación electrónica de datos, con la consecuente trasgresión de las seguridades dispuestas por el 'Webmaster' o prestador del servicio al *'Webhosting'* u 'Owner', con el fin de proteger los servicios de transmisión, almacenamiento y procesamiento de datos que ofrece frente a posibles abusos de terceros (ingreso en cuentas de e-mail ajenas). Así como también la utilización o interferencia indebidos de dichos equipos o sistemas informáticos o telemáticos, o la permanencia contumaz en los mismos por fuera de la autorización o del consentimiento válidamente emitido por el titular del derecho. (Posada Maya, 2006b, p. 23)[14].

Este tipo de comportamientos punibles constituyen verdaderas conductas preparatorias o preliminares de infracción a la seguridad y al control informático (Quintero Olivares & Morales Prats, 2011a, pp. 481, 483), de peligro y de ejecución abierta que, por lo general, acompañan a la mayoría de conductas delictivas sancionadas por el legislador colombiano como parte de la cadena de ataques a un determinado sistema informático o a los datos e información almacenados en este.

En el ordenamiento penal colombiano, a diferencia de otros ordenamientos penales como el español[15], el italiano[16] o el alemán[17], el delito

12 Esta figura delictiva tiene antecedentes doctrinales en la Convención de Budapest (2003), cap. I, art. 2, en los siguientes términos: "Acceso ilegal. 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 intención delictiva, o también podrán requerir que la infracción se perpetre en un sistema informático conectado a otro sistema informático" (t. l.). Normativa que se asemeja al *Misuse Act* de 1990, *Section* 1 (1) de Gran Bretaña.

13 Con ello no se pretende hacer referencia a la conducta de intrusión en un ámbito profesional, sino a las conductas que atentan contra la intimidad informática realizadas en calidad de 'intruso' o 'extraño'.

14 Morón Lerma (2002, pp. 51).

15 El CP español consagra la figura de acceso abusivo a datos o programas en el art. 197.3 adc. L. O. 5/2010, del siguiente modo: "El que, por cualquier medio o procedimiento y vulnerando las medidas de seguridad establecidas para impedirlo, acceda sin autorización a datos o programas informáticos contenidos en un sistema informático o en parte del mismo o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo ejercicio a excluirlo, será castigado con la pena de prisión de seis a dos años". En particular, obsérvese que dicha norma prevé la exigencia de medidas de seguridad y que el sujeto debe obtener algún tipo de información reservada. En la doctrina v. Anarte Borallo (pp. 225 y ss.); Boix Reig & otros (2010, pp. 454 y ss.); Morillas Cueva (2011, pp. 319 y ss.); Polaino Navarrete & otros (2010, p. 237); Quintero Olivares & Morales Prats (2011a, pp. 481 y ss.); Quintero Olivares & Morales Prats, artículos 1 a 233 (2011, pp. 1321 y ss.); Rodríguez Moro (2011, pp. 248 y ss.); Salvadori (2011a, pp. 767 y ss.) tiene versión española: Salvadori (2011b, pp. 221 y ss.).

16 El CP italiano consagra en el art. 615*ter*, la figura de acceso abusivo a un sistema informático e telemático (L. n. 547/1993): "Quien abusivamente se introduzca en un sistema informático o telemático protegido por medidas de seguridad o se mantenga en él contra la voluntad expresa o tácita de quien tiene el derecho de excluirlo, será castigado con prisión hasta de tres años" (T. L.), como una modalidad del delito de violación de domicilio. A diferencia de este, el texto colombiano no cubre los sistemas telemáticos y no requiere el conocimiento posterior de datos personales. En la doctrina italiana v. Mantovani (2008, pp. 520 y ss.); Del Pino (2009, p. 585) y Salvadori (2012, p. 370 y en particular la 390).

17 El StGB alemán consagra el tipo penal de espionaje de datos informáticos (Ausspähen von Daten) en el § 202(a) (2. WiKGvom 15.5.1986,

de acceso abusivo a un sistema informático no se clasifica como una modalidad de *espionaje informático* (porque no se exige de *lege data* el conocimiento o la disposición de datos: 'cracking malicioso') ni del delito de *violación de habitación ajena*, por más que, en el último caso, se trate de equiparar los conceptos de sistema informático y domicilio, con el argumento —por cierto muy dudoso— de que se busca proteger el domicilio informático del titular del bien jurídico. No es claro que tal cosa sea posible en el ámbito virtual, como un concepto distinto a la noción de dominio informático[18].

Véanse a continuación los elementos objetivos y subjetivos de la figura:

A. Aspecto objetivo

1. sujeto activo

Monosubjetivo y común indeterminado: "*El que*": cualquier persona natural que realice la acción propia del tipo penal de *acceso abusivo a sistema informático*, sin que este requiera alguna calificación especial. Dicho en otras palabras, el sujeto no tiene por qué ser un *hacker* o un *cracker*[19] profesional, basta que sea un "intruso" y se cumplan las exigencias jurídicas para ser calificado como autor. Es más, hay que tener en cuenta que el mismo prestador del servicio puede ser autor cuando, sin legitimidad jurídica y arguyendo razones de verificación, ingresa a un sistema informático protegido o no como, por ejemplo, el correo electrónico de sus usuarios, siempre que este uso no se haya estipulado expresamente en las normas de uso o administración (García, González, 2006, pp. 297 y ss.).

El sujeto activo y su actuación informática pueden ser rastreados e identificados a partir de la IP que ha desencadenado el ataque contra el sistema informático, acompañado del número MAC (o serial del hardware de conexión), como emisor y receptor de la información que busca concretar la acción punible[20].

Este tipo penal admite la coautoría y otras formas de autoría, y las diversas formas de participación criminal: (i) determinación y (ii) complicidad (CP, arts. 29 y 30).

mod. 41 StÄGvom 7.8.2007), en Nomos Gesetze (2011): "Quien se procure para sí o para otro el acceso a datos que no estén particularmente asegurados contra un acceso ilícito, o que se consigan con la vulneración de un acceso de seguridad, será castigado con una pena privativa de libertad de hasta tres años o con pena de multa" (T. L.). Sobre la interpretación de esta figura v. Kindhäuser (2009, pp. 211-212); Krey, Heinrich & Hellmann (2012, pp. 205-213); Rengier (2011, p. 250); Schmidt & Priebe (2010, p. 294) y Wessels & Hettinger (2011, pp. 170-171).

18 En contra de esta asimilación, precisamente por comportar más problemas que ventajas teóricas y prácticas, v. Posada Maya (2006b, p. 23).

19 Cfr. sobre este concepto: González Rus (2006, pp. 258-259); Quintero Olivares, Morales Prats & otros (2011b, pp. 1306-1307), artículos 1 a 233; Rovira del Canto (2002, p. 130); Rueda Martín (2009, p. 158).

20 Según es.Wikipedia.org: "Una dirección IP es una etiqueta numérica que identifica, de manera lógica y jerárquica, a un interfaz (elemento de comunicación/conexión) de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo IP (*Internet Protocol*), que corresponde al nivel de red del Modelo OSI. Dicho número no se ha de confundir con la dirección MAC, que es un identificador de 48 bits para identificar de forma única la tarjeta de red y no depende del protocolo de conexión utilizado ni de la red. La dirección IP puede cambiar muy a menudo por cambios en la red o porque el dispositivo encargado dentro de la red de asignar las direcciones IP decida asignar otra IP (por ejemplo, con el protocolo DHCP). A esta forma de asignación de dirección IP, *dirección IP dinámica* (normalmente abreviado como *IP dinámica*). / Los sitios de Internet que por su naturaleza necesitan estar permanentemente conectados generalmente tienen una *dirección IP fija* (comúnmente, *IP fija* o *IP estática*). Esta no cambia con el tiempo. Los servidores de correo, DNS, FTP públicos y servidores de páginas web necesariamente deben contar con una dirección IP fija o estática, ya que de esta forma se permite su localización en la red. / Los ordenadores se conectan entre sí mediante sus respectivas direcciones IP. (…)".

Asimismo, hay que tener en cuenta que el CP, art. 269H, modifica y agrava el tipo penal de la mitad a las tres cuartas partes, cuando el sujeto activo tenga las siguientes calidades:

a) *Servidor público en ejercicio de sus funciones* (num. 2 *ibidem*). Incremento punitivo que se fundamenta en la mayor exigibilidad que comporta tal cualificación, al ejecutar el acceso con abuso del cargo o de la función pública. En caso de haber un acto de espionaje adicional, según el caso, se aplicaría el tipo penal vertido en el CP, art. 269C o en el art. 269F. El tema se resuelve en sede de concursos aparentes.

b) *Cuando el sujeto activo pueda ser considerado como un insider* (num. 8 *ibidem*), esto es, cuando el sujeto sea el responsable de la *administración* —administrar: 3. tr. Ordenar, disponer, organizar, en especial la hacienda o los bienes—, *manejo* —manejar: 4. Gobernar, dirigir— o *control* —1. m. Comprobación, inspección, fiscalización, intervención. 2. m. Dominio, mando, preponderancia—[21] del sistema informático. En el último caso, el legislador decidió imponer también, como sanción principal privativa de derechos, la pena de *inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos informáticos,* por el mismo tiempo que dure la pena privativa de la libertad. Esta calificación como *insider* es igualmente recogida por el num. 2 del art. 269H, al castigar al sujeto que actúa prevaliéndose de una relación contractual previa para ejecutar, por ejemplo, los actos de acceso o de mantenimiento del sistema. Relación que definirá, como se dirá más adelante, los límites dentro de los cuales puede obrar un determinado sujeto sin que su comportamiento se pueda considerar abusivo.

En todo caso, la calificación del sujeto activo conlleva un complejo debate en la doctrina, porque, si bien pocos autores discuten que el tipo penal fundamental está diseñado primordialmente para que un extraño u *outsider* ejecute el acceso abusivo *ex novo* al sistema informático, o luego de un acceso casual se mantenga en el sistema, no ocurre lo mismo con el sujeto *insider.* Precisamente, algún sector de la doctrina especializada debate ampliamente si cabe aplicar esta figura tratándose de sujetos *insider*, es decir, personas que en principio están autorizadas por el titular para acceder al sistema informático. Así, por ejemplo, Salvadori (2011, pp. 371 y 372) señala que en estos casos la aplicación de la agravante supondría una violación al principio del *ne bis in idem*, porque, en los casos de permanencia abusiva, la misma condición de *insider*, esto es, el hecho de estar previamente habilitado para acceder al sistema informático, ya sería una condición inherente para ser considerado como sujeto activo del tipo penal fundamental.

Por el contrario, la doctrina mayoritaria sostiene, y ello parece lo correcto, que sí es posible que un sujeto *insider* acceda a un sistema informático de manera abusiva. Precisamente, puede suceder que el sujeto activo solo tenga una autorización para ingresar al sistema, pero este se mantenga en contra de la voluntad expresa del titular, bien porque solo estaba autorizado para realizar actividades o tareas específicas (de re-

21 Todas las voces han sido consultadas en www.rae.es

paración, uso de cierto software o consulta de la Internet, y no para copiar programas o para borrarlos); bien porque únicamente podía permanecer durante un específico período de tiempo o durante ciertos días; o, en fin, solo podía acceder a cierta parte del sistema, con lo cual, el hecho de mantenerse por fuera de las condiciones autorizadas resulta claramente abusivo, es decir, no autorizado.

Así las cosas, en ambas hipótesis, cuando las mencionadas condiciones de autorización son excedidas o desconocidas, quien antes se consideraba un *insider* legítimo se convierte en un insider ilegítimo (*outsider*) o intruso dentro del sistema informático. Como se dirá más adelante, el asunto a verificar con exactitud sería la fuerza y el alcance de la fuente jurídica que determina la legalidad (o legitimidad) de la actuación del sujeto activo del tipo en el caso concreto.

2. Sujeto pasivo

Común, monosubjetivo y colectivo: solo pueden ser sujetos pasivos de este tipo penal aquellas personas que sean, por una parte, el titular del medio informático que resulta objeto del acceso o mantenimiento abusivo, que incluso puede ser una persona jurídica, y, por la otra, el titular de los datos personales, sensibles o secretos almacenados en archivos o bases de datos, y cuya intimidad personal se pone en peligro (Fernández Teruelo, 2011, pp. 195 y ss.; Queralt Jiménez (2010, p. 302).También será sujeto pasivo, en sentido colectivo, la comunidad como titular del bien jurídico seguridad de la información y de los datos, en particular de la seguridad de las funciones informáticas (idoneidad, autenticidad y disponibilidad)[22].

3. Bien jurídico

Este tipo penal pluriofensivo (Rovira del Canto, 2002, p. 187) exige, en primer lugar, la afectación o vulneración del bien jurídico intermedio, público y autónomo de *la seguridad de la información y los datos informáticos*[23], con lo cual se sanciona la lesión de *la confiabilidad, integridad y la libre disponibilidad directa de los sistemas informáticos y el peligro indirecto de los datos y la información*[24] almacenada en ellos.

En cuanto a la lesión del sistema informático, autores como (Rueda Martín, 2009, p. 182) señalan:

> Pero también hay que constatar que con tales comportamientos se produce la lesión de la confidencialidad, integridad y disponibilidad de los sistemas informáticos mediante el simple acceso a los mismos, tanto si se realiza con la finalidad de descubrir fallos o puertos falsos en dichos sistemas informáticos que alberguen archivos de datos reservados. Según esta estruc-

22 Es necesario subrayar que estas calidades, referidas a las características de los objetos sobre los cuales recae la acción punible, tienen un sentido distinto a la idoneidad, autenticidad y suficiencia que requieren los datos informáticos para servir como evidencia digital en un proceso judicial. Sobre este último aspecto v. Cano M. (2009, pp. 109 y ss.).

23 Sobre el tema del bien jurídico, v. ampliamente Posada Maya (2013, pp. 7 y 8).

24 Por su parte, Picotti (2006a, p. 350), sostiene que la simplificación típica supone, respecto al espacio informático, poner "[…] en primer plano la exigencia de la tutela del interés *colectivo* a la protección de la legitimidad de cada acceso a cualquier punto de la red, frente a la extensión global de las interconexiones vía Internet, para garantizar la seguridad de todos, y sostener la idea de que se trate de tutelar sólo el *jus excludendi* del individuo, así como de depositar confianza en su diligencia o capacidad subjetiva para la protección del propio sistema […]".

> tura, si bien es deseable la previsión de alguna finalidad ulterior de atacar los datos, como se dirá más adelante, el sistema se protege con independencia de su contenido.

Más adelante (p. 187), agrega:

> De esta manera cuando un hacker penetra ilícitamente en un sistema informático ajeno, tanto si se han infringido medidas de carácter técnico como si no ha sido así, se encuentra en un espacio, el propio sistema, en el que su integridad se ha visto afectada porque la sola entrada y el consiguiente uso del sistema da lugar a modificaciones en los datos del mismo, junto con las alteraciones de tales datos para intentar borrar los rastros que pudieran identificarles (...).

En segundo lugar, el tipo penal exige también la puesta en peligro del bien jurídico personalísimo de la *intimidad personal*[25] en su modalidad de la *intimidad y la autodeterminación informáticas* —igualmente considerado como un derecho fundamental de cuarta generación (Anarte Borallo, p. 236)—, para evitar potenciales lesiones a los datos de naturaleza privada o semiprivada (Picotti, 2006, pp. 181 y ss.)[26] y a la información informatizada almacenada en el sistema objeto de ataque, mediante acciones ulteriores o manipulaciones informáticas que, más allá, puedan configurar un delito autónomo de interceptación o violación de datos personales (CP, arts. 269 C y F, respectivamente). Por esto, se trata de un bien jurídico colectivo-individual.

Por su parte, Fiandaca & Musco (2007, p. 199) y Salvadori (2012, p. 391) se refieren a la disponibilidad exclusiva del espacio informático. De la potencial confianza y expectativa de intimidad informática del sujeto pasivo respecto de la incolumidad e inviolabilidad de los datos personales[27] e informaciones informatizados,

25 La Corte Constitucional (en adelante CConst.), señala en la sent. C-913 de 2010 sobre la intimidad en sentido negativo, que "El núcleo esencial del derecho a la intimidad, supone la existencia y goce de una órbita reservada en cada persona, exenta de poder de intervención del Estado o de las intromisiones arbitrarias de la sociedad, que le permita a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural"; SU-056 de 1995: "El derecho a la intimidad hace referencia al ámbito personalísimo de cada individuo o familia, es decir, a aquellos fenómenos, comportamientos, datos y situaciones que normalmente están sustraídos a la injerencia o al conocimiento de extraños. Lo íntimo, lo realmente privado y personalísimo de las personas es, como lo ha señalado en múltiples oportunidades esta Corte, un derecho fundamental del ser humano, y debe mantener esa condición, es decir, pertenecer a una esfera o a un ámbito reservado, no conocido, no sabido, no promulgado, a menos que los hechos o circunstancias relevantes concernientes a dicha intimidad sean conocidos por terceros por voluntad del titular del derecho o porque han trascendido al dominio de la opinión pública". Agrega la T-814 de 2003, que "el ámbito de protección de la intimidad varía dependiendo de las personas, pues en ejercicio de su libertad individual éstas deciden hacer públicos distintos aspectos de su vida. Sin embargo, más allá de lo que atañe al derecho a la intimidad, la naturaleza de la información afecta en mayor o menor medida a las personas debido al valor atribuido socialmente a los distintos aspectos de la vida en comunidad." La extensa jurisprudencia puede ser consultada en: http://www.corteconstitucional.gov.co/relatoria/tematico.php?todos%22=%25&sql=intimidad&campo=%2F&pg=0&vs=0

26 Posada Maya (2006a, p. 57), desde entonces se entendía que el ordenamiento nacional protegía la privacidad informática. En la doctrina v. Polaino Navarrete & otros (2010, p. 238).

27 La L. E. 1581 de 2012, art. 3°, define el dato personal como "cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables" y en el art. 5 el dato sensible, así: "Para los propósitos de la presente ley, se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promuevan intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos". Definiciones que también deben cubrir a las personas jurídicas. Cfr. CConst., sent. C-1011 de 2008, Finalmente, el Convenio de Budapest de 2003, entiende por datos o información en el Ch. I, art. 1°, aquella "unidad básica de información, ello es, cualquier representación de información, conocimiento, hechos, conceptos o instrucciones que pueden ser procesadas u operadas por sistemas automáticos de computadores, y cuya unión con otros datos conforma la información en sentido estricto". La característica esencial es que este tipo de elementos no son susceptibles de visualización directa y para ello requieren un procesamiento digital que haga explícitas las señales que los integran. En cuanto a los datos personales, estamos de acuerdo con Anarte Borallo (2003, p. 247) cuando indica que "De acuerdo con ello, no es su contenido inmediato ideológico, religioso, racial, sexual o relativo a la salud individual lo que determina la cualificación, sino su

almacenados y tratados en estos, su confiabilidad, disponibilidad y seguridad hablan De la Cuesta Arzamendi & otros (2010, p. 47) y Cano M. (2009, pp. 108 y ss.). Por su parte, Mantovani (2008) retoma el castigo a la indiscreción informática o telemática y subraya el deber de prevenir el hurto de servicios informáticos.

En todo caso, teniendo en cuenta que este tipo de presunciones de *iure* en los tipos de peligro son esencialmente desproporcionadas y lesivas de garantías fundamentales como la *ofensividad material*[28], resulta necesario reinterpretar la figura como un delito de peligro en concreto (CP, art. 11), en el entendido de que se requiere verificar un *peligro efectivo* contra los bienes jurídicos protegidos por la norma penal (Posada Maya, 2006b, pp. 29 y 30)[29].

4. Objeto jurídico

El objeto jurídico del tipo penal de *acceso abusivo a sistema informático* consiste en proteger, en concreto, el derecho o facultad de control del titular sobre la *integridad* y *seguridad* del sistema informático[30], el derecho personalísimo a la autodeterminación informática[31], y a ejercer, derivado de estos derechos, el *jus excludendi* frente a terceros que intenten acceder de manera arbitraria, fraudulenta o violenta al sistema.

Esta facultad de control se traduce en varias atribuciones concretas, susceptibles de protección: 1) requerir previa autorización o consentimiento del titular para el acceso y el uso de un sistema informático; 2) saber y ser informado sobre el uso dado al sistema informático; 3) orientar, corregir, excluir, etcétera, las condiciones de uso y el uso efectivo de un sistema informático; y 4) el derecho a mantener protegido el sistema informático y a que nadie interfiera con dicha protección informática. Estos derechos surgen con independencia de la calidad de los datos que se encuentren almacenados en el sistema[32].

En estas condiciones, aunque de manera subsidiaria, también se protegen el derecho a "la regularidad del funcionamiento" de los sistemas informáticos, y la reserva que debe acompañar la utilización de sus recursos (lo que incluye el uso del software).

Ahora bien, los sistemas informáticos pueden "residir" en Colombia o en el exterior —lo que dependería del sitio en donde esté el correspondiente servidor—; es más, incluso es posible que el sistema virtual se encuentre en la nube (*cloud*). Lo importante es que el sujeto activo

aptitud, apreciable también en concreto, para desvelar esos aspectos de la vida de una persona".

28 V. Quintero Olivares, Morales Prats & Otros (2011b, p. 1306) artículos 1 a 233 y Boix Reig & otros (2010, p. 456) se refieren a esta figura como un "abstracto delito de peligro".

29 Desde luego, no faltan autores que consideran que el tipo penal solo es de lesión efectiva (Rey Boek & Nuñez de León, 2011, pp. 632-633).

30 En el mismo sentido: Boix Reig &otros (2010, p. 455), Rodríguez Moro (2011, p. 248), Velasco San Martín (2012, p. 55).

31 Anarte Borallo (2003, pp. 228, 237-238), Quintero Olivares, Morales Prats & Otros (2011, pp. 1293-1298) artículos 1 a 233.

32 L. E. 1581 de 2012/art. 8. "El Titular de los datos personales tendrá los siguientes derechos: c) Ser informado por el Responsable del Tratamiento o el Encargado del Tratamiento, previa solicitud, respecto del uso que le ha dado a sus datos personales; e) Revocar la autorización y/o solicitar la supresión del dato cuando en el Tratamiento no se respeten los principios, derechos y garantías constitucionales y legales. La revocatoria y/o supresión procederá cuando la Superintendencia de Industria y Comercio haya determinado que en el Tratamiento el Responsable o Encargado han incurrido en conductas contrarias a esta ley y a la Constitución".

del tipo realice los actos de manipulación (en sentido amplio) o dicte sus instrucciones intrusivas desde Colombia, para que se pueda aplicar el derecho penal nacional, lugar en el que ha iniciado la acción que produce el riesgo jurídicamente desaprobado, en términos de la imputación objetiva (CP, art. 26).

5. Objeto sobre el cual recae la acción

Inmaterial determinable: el objeto sobre el cual recae la acción del delito previsto en el art. 269A puede ser definido en sentido general y en sentido concreto. En sentido general el objeto sobre el cual recae la acción informática es el *sistema informático*, entendido como un dispositivo o un grupo de dispositivos informáticos individuales interconectados entre sí que realizan acciones de tratamiento, procesamiento y almacenamiento automático de datos[33]. En estricto sentido el objeto *inmaterial* sobre el cual recae la acción de acceso abusivo serían los sistemas operativos o aplicativos —software— que permiten procesar u operar automáticamente instrucciones o datos contenidos en ficheros o archivos. El tipo penal estudiado, a diferencia de otras figuras delictivas previstas en la ley colombiana, no protege directamente los datos o la información informatizada personal contenidos en estos. Solo lo hace de manera indirecta o potencial.

De otra parte, la norma legal señala que el sujeto activo puede acceder *a todo o en parte* del sistema, esto es, a determinados programas aplicativos o a ciertos ficheros o bases de datos. Por el contrario, no quedan comprendidos otros elementos *físicos* del sistema como objetos jurídicos concretos, porque estos no suponen una configuración técnica idónea o capaz de admitir accesos informáticos o lógicos.

Asimismo, todo indica que la descripción típica tampoco cubre los actos de acceso contra los *sistemas telemáticos*. Los sistemas informáticos almacenan y procesan datos o información, mientras que los sistemas telemáticos están compuestos por elementos que sirven para la trasmisión y comunicación de datos a distancia o en redes (Mantovani, 2008, p. 520). Asimilar ambos sistemas constituiría una analogía *in malam partem* prohibida por la CN, art. 29 y por el CP, art. 6°.

Finalmente, hay que tener en cuenta que el art. 269H, num. 1, permite agravar la pena consagrada para los artículos previstos en el título, de la mitad a las tres cuartas partes, cuando la acción recaiga "1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros". Se trata de una protección sobre consideraciones de política-criminal, dada la importancia y la función que cumplen este tipo de objetos-medio oficiales en comparación con los sistemas informáticos privados o particulares. Asimismo, en algunos eventos, cuando se vulneran otros bienes jurídicos colectivos como la seguridad nacional y defensa del Estado (num. 6), se advierte un mayor desvalor de resultado en la ejecución del delito.

33 En el mismo sentido v. Pabón Parra (2011, p. 500).

6. Verbo rector mixto de conducta alternativa

El tipo vertido en el art. 269A es mixto de conducta alternativa y puede ser realizado, bien a) accediendo a un sistema informático o b) manteniéndose dentro de este en contra de la voluntad de quien tenga derecho a excluirlo. Derecho que tiene que ser cierto, legítimo y preexistente al abuso del sistema informático.

a) *El acceso a sistema informático*. Por tal se entiende la acción de *acceder ex novo* —3. intr. Entrar en un lugar o pasar a él[34]— de manera directa, indirecta o remota a un sistema informático, con el cual el sujeto activo traba un diálogo lógico claramente abusivo o no autorizado. Esta modalidad típica es de mera conducta o pura actividad, y de consumación instantánea cuando se produce la simple introducción o acceso. En cuanto a su ofensividad, se remite a los conceptos de bien jurídico y objeto jurídico protegidos ya señalados.

El acceso tiene que ser informático o virtual, no puede ser físico (Del Pino, 2009, p. 586)[35]. Según Salvadori (2012, p. 376), el acceso "se realiza mediante la digitación de una serie de comandos con los cuales se ordena a un sistema informático ejecutar una determinada operación y esta, respondida en sentido positivo, le permite al sujeto solicitante utilizar en todo o en parte sus recursos" informáticos.

Sobre el particular, al analizar las técnicas básicas y avanzadas de Hacking (Cano M., 2009, p. 35 y ss. y 43 y ss.), señala que el *iter criminis* de este tipo de conductas usualmente se compone de tres fases, a saber: i) la etapa de *reconocimiento*, ii) la fase de *vulneración,* y iii) la fase de *eliminación y salto*. En la fase de reconocimiento, el atacante hacker "(...) hace un escenario de riesgos actuales y emergentes a los que está expuesto el objetivo, para, sobre este plano de incertidumbre identificado, poder avanzar en situaciones que desestabilicen el orden de las operaciones y actividades del objetivo" (p. 36). La fase de reconocimiento comporta verdaderos actos preparatorios de espionaje, dentro de los cuales se advierte, por ejemplo, averiguar las características del equipo a acceder, los datos necesarios para el ingreso (violación de datos) o datos que le permitan al hacker o cracker desarrollar modelos o esquemas de ataque cibernético, etcétera.

La segunda fase del ataque consiste en la vulneración del sistema. Esta se estructura por aquellos comportamientos que realmente sanciona el delito de acceso abusivo a un sistema informático, porque "implica comprometer el sistema, escalar y avanzar hasta el nivel más alto de privilegios permitido, y mantener el control del sistema atacado, o sencillamente inutilizar y generar pérdida de disponibilidad del sistema bajo hostigamiento" (p. 37). Actividades que usualmente son clandestinas, rápidas y para las cuales se emplean sofisticados programas y técnicas de evasión y eliminación de rasgos que impidan descubrir la "trazabilidad" de la injerencia en el sistema[36]. Finalmente, la fase

34 Consultado en www.rae.es. En la doctrina v. Morillas Cueva (2011, p. 319), Rodríguez Moro (2011, p. 249).

35 En contra, Queralt Jiménez (2010, p. 32) afirma que el acceso también puede ser físico.

36 Cano Martínez (2009, p. 104). También en Cano Martínez (2010, pp. 240 y ss.).

tres consiste en anular o evadir los mecanismos de monitoreo y de control, y normalizar la presencia del hacker en el sistema. A partir de allí es posible realizar otro tipo de actividades utilizando otros programas maliciosos o no, pero sin perder los beneficios o privilegios que el acceso abusivo le ha concedido al hacker.

Ahora bien, cuando se afirma que el acceso informático debe ser *abusivo* o con violación de las condiciones de privacidad de la información, se quiere expresar que el sujeto activo debe carecer de la autorización o del consentimiento expreso del titular del sistema informático o de aquella persona que tiene la capacidad para otorgar ese consentimiento de manera válida y lícita, en los términos del CP, art. 32, num. 1°, para ingresar o mantenerse en el medio.

Consentimiento que constituye, para los efectos del comportamiento estudiado, una causal de ausencia de tipicidad que anula la desaprobación *ex ante* de cualquier acto de intrusión. La conducta también será abusiva cuando el sujeto activo acceda al sistema informático en contravía de las condiciones previamente acordadas con el titular (como en el caso de existir una relación contractual, lo que además agravaría la tipicidad según el CP, art. 269H, num. 2).

Finalmente, para matizar la cuestionada presunción *iure et de iure* con respeto a la lesión potencial del bien jurídico *intimidad informática*, es necesario exigir que el comportamiento represente, cuando menos, un peligro concreto frente a la integridad, seguridad y la reserva o privacidad de los datos almacenados en el sistema. Peligro verificable y concreto que existiría cuando el sujeto tenga "la posibilidad fáctica —*al menos un instante*— de obtener servicios o de disponer de la información existente y retirarla del mismo [...]" (Posada Maya, 2006b, p. 24), a condición de que dicha información o datos almacenados sean sensibles para el titular o terceros.

b) *El mantenerse dentro del sistema*. Esta modalidad de mera conducta, también denominada como *permanencia abusiva*, tiene lugar cuando el sujeto activo, si bien accede al sistema informático de manera lícita o legítima, o en forma accidental o no intencional, mantiene[37] un diálogo o nexo lógico con el sistema informático —*se mantiene o prosigue conectado*—, en contra de la voluntad concurrente del titular con derecho legítimo a excluir a terceros (*jus excluendi*), para proteger las condiciones de integridad, confiabilidad, disponibilidad y privacidad del medio informático. Permanencia que debe darse con la conciencia de que no se está autorizado y que ello constituye un abuso informático.

A diferencia del verbo rector "acceder", el verbo rector mantenerse es de *ejecución permanente*[38], en el sentido de que la actividad antijurídica de proseguir el nexo lógico cesa cuando el sujeto activo sale del sistema informático y termina todo tipo de diálogo abusivo (*log-out*), o cuando es excluido exitosamente por el sujeto pasivo, lo que conlleva la terminación del tipo penal.

La voluntad de exclusión del titular debe manifestarse de manera expresa e inequívoca (aun-

37 Consultado en www.rae.es — "5. tr. Proseguir en lo que se está ejecutando", lo que significa que es un hacer en español. En la doctrina v. Quintero Olivares & Morales Prats (2011a, p. 485).

38 En sentido similar v. Pabón Parra (2011, p. 499).

que en otros ordenamientos jurídico-penales pueda ser *tácita*, como en el CP italiano, art. 615*ter*), por lo que debe existir una advertencia previa al sujeto activo por parte del sujeto pasivo o su equivalente, para que el autor no dude de que está actuando como un extraño que se mantiene en forma contumaz. Advertencia que cobra especial importancia en las hipótesis de ingreso accidental o casual, en las que el sujeto activo podría alegar que actuó bajo un error sobre los presupuestos del consentimiento (CP, art. 32, núm. 10 en concordancia con el art. 32, núm. 2), si no conoció que su permanencia voluntaria contrariaba claramente la voluntad del titular legítimo[39]. Dicha advertencia, señal o alarma previa no tiene por qué ser informática.

c) *Sobre las dos modalidades típicas expuestas es necesario efectuar varias consideraciones*:

En primer lugar, a diferencia del tipo penal original previsto en el art. 195 del CP —der. L. 1273 de 2009, art. 4°—, la conducta típica vigente de *acceso o mantenimiento abusivo* (CP, art. 269A) no tiene por qué recaer sobre un objeto inmaterial calificado o cerrado. Dicho en otras palabras, el legislador penal colombiano decidió —de manera desacertada— que es irrelevante si el sistema informático (objeto-medio) estaba previamente "protegido o no" con una medida de seguridad informática idónea y eficaz, según los estándares comunes de gestión en seguridad informática; medidas dispuestas por el titular del bien jurídico para limitar expresamente el 'ingreso' o acceso libre al sistema informático, programa o módulo informático o base de datos[40]. Resulta absurda, entonces, la inclusión de la expresión "protegida o no" con medida de seguridad, que bien puede ser suprimida de la redacción típica actual.

Desde otra perspectiva, lo dicho significa que, a efectos del tipo penal nacional, no interesa si el sujeto activo ha realizado manipulaciones de naturaleza informática dirigidas a superar tales medidas de seguridad. Y menos si el sujeto activo tiene conocimientos especiales para superar tal tipo de medidas o si utilizó aparatos electrónicos para ello —no así si utilizó software malicioso, porque se adecuaría al tipo penal previsto en el CP, art. 269E, en su modalidad de introducir programas maliciosos al sistema informático—. Por tal motivo, bastaría utilizar un sistema al que otro sujeto ha accedido previamente, para que se consume el tipo penal.

En todo caso, la eliminación de la medida de seguridad permite considerar típico un acceso a un sistema de seguridad completamente desprotegido por su titular (abierto) o con baja o reducida expectativa de intimidad, incluso por negligencia o voluntad de su dueño, siempre que este no sea de acceso libre o público, o cuando no preexista un acto de autorización o consentimiento previo por parte de su dominio.

Por ejemplo, piénsese en el caso de que A encuentre una tableta perdida en el campus de la

39 En todo caso, es muy importante que dentro del proceso penal se acredite, de manera precisa, la calidad de la persona que puede otorgar de manera legítima el consentimiento, de lo contrario se generaría una duda probatoria acerca de la existencia o inexistencia o de la validez del consentimiento en el juicio.

40 Con una postura contraria, que no se compadece con la reforma del 2009, v. Arboleda Vallejo & Ruiz Salazar (2012, p. 1020).

universidad, y (aunque esta esté o no protegida) el sujeto ingresa al sistema operativo para verificar la identidad de su legítimo propietario con el fin de entregarla o restituirla. Ejemplo que en principio sería típico, no solo por la absurda redacción de la norma, sino también por tratarse de un tipo penal de peligro que de manera indirecta protege la confianza o la expectativa de intimidad del sujeto pasivo, aunque los datos allí contenidos no sean de alta prioridad para este.

Se castiga como acceso abusivo, entonces, el acceso o mantenimiento dentro de sistemas de seguridad desprotegidos, asunto que tendrá especial consideración político-criminal cuando se analice la imputación objetiva, y en particular figuras como la *auto-puesta en peligro* de los sistemas o de la información dentro del denominado *suicidio informático*.

Otro cuestionamiento acerca de la eliminación de las medidas de seguridad informáticas, como elemento del tipo penal, tiene relación con que el derecho penal colombiano ya no considera que el titular de la información sea, en primera instancia, el principal responsable de su protección, según la importancia que se le otorgue a esta. Con el tipo penal original, la doctrina nacional razonó que un sistema desprotegido era un sistema asimilado a los sistemas informáticos abiertos, precisamente porque la falta de protección (medidas informáticas idóneas) señala de manera inequívoca el poco interés del titular del sistema para reservar la disponibilidad, integridad y confidencialidad de los datos o de la información almacenada. Así, con la eliminación del elemento normativo mencionado, el legislador penal le dio carta blanca a la irresponsabilidad del titular, de tal manera que sea este diligente o negligente al proteger el sistema (PC, Smartphone, cajero electrónico, etcétera), siempre habrá acceso punible cuando alguien ingrese al sistema. Cede por consiguiente el principio político-criminal de autorresponsabilidad informática respecto de la tenencia de información sensible.

En segundo lugar, la dogmática penal moderna discute sobre la clase de conducta que comportan las modalidades típicas estudiadas. Si bien no hay duda de que el acceso —directo o remoto— a un sistema informático es una modalidad comisiva, no existe consenso en relación con la clase de conducta que comporta el hecho de *mantenerse* dentro del sistema informático de manera contumaz.

a) Una primera postura teórica cree que 'mantenerse' dentro del sistema es una conducta omisiva pura, por medio de la cual el sujeto activo infringe dolosamente, al no salir del sistema (no hacer *log-out*), un mandato de abandono que ha sido planteado en forma expresa o tácita por parte del titular legítimo. Para los expertos, la cuestión principal radica en determinar la clase de deber legal que precede a la omisión (pura) de abandono y su fuente legal[41].

41 En este sentido v. ampliamente, Salvadori (2012, p. 378; 2011, pp. 232 y 233) quien agrega en esta última que "La conducta (alternativa) de mantenerse en un sistema incluiría, por lo tanto, las hipótesis omisivas de la "parada" o de la "permanencia" abusiva en un sistema informático, que no podrían ser de otra manera subsumidas en la conducta activa de "acceso" no autorizado". No obstante, a renglón seguido agrega: "Esta conducta no tendrá que entenderse en sentido "físico", sino como mantenimiento de la conexión, inicialmente obtenida de manera autorizada o fortuita, a todo o en parte de un sistema de información. Lo que se castiga por lo tanto es la "permanencia" *invito domino* en el sistema informático ajeno realizada por quien, por casualidad o teniendo al principio la autorización del legítimo titular, haya seguido manteniéndose en el sistema informático pese a que haya acabado el consentimien-

Para esta corriente doctrinal, esta variante del tipo se consumaría a partir del momento en el cual surge la obligación de terminar la conexión lógica con el sistema informático[42], lo que tiene como consecuencia que el sujeto que accede al sistema deja de ser huésped y se convierte en un extraño.

Varios son los inconvenientes de esta teoría para nuestro medio, determinados por los postulados de legalidad (CP, art. 6°) y de taxatividad (CP, art. 10°), advirtiendo que las omisiones propias se rigen por un sistema de *numerus clausus*:

Primero, todo indica que la protección de la *seguridad de la información, los datos y los sistemas informáticos* no puede ser cubierta, en Colombia, mediante tipos penales de comisión por omisión en los que el deber de garante deba encontrar soporte en fuentes materiales, ya que —infortunadamente— el parágrafo del art. 25 CP limita estas fuentes (los numerales enunciados a título de ejemplo del 1 al 4) a los tipos que castiguen por comisión las conductas punibles contra "la vida e integridad personal, la libertad individual, y la libertad y formación sexuales". Además, es obvio que el art. 269A no es un supuesto de comisión por omisión, porque el debate se presenta frente a un verbo rector expreso que no exige un resultado típico de naturaleza material que lesione el bien jurídico protegido. Dicho en otras palabras, el tipo vertido en el art. 269A es de mera conducta y no de resultado material y, además, es claramente comisivo.

Segundo, en Colombia, los mandatos normativos (imperativos) *concretos* que fundamentan los delitos de omisión propia deben tener categoría legal. No otra cosa se desprende del art. 10 *ibidem*, inc. 2°, cuando señala que "En los tipos de omisión también el deber tendrá que estar consagrado y delimitado claramente en la Constitución Política o en la ley"[43] (Velásquez Velásquez, 2009, pp. 663 y 67) y de la LE 1581 de 2012/art. 4°. *Principios para el Tratamiento de datos personales. "*a) Principio de legalidad en materia de Tratamiento de datos". Según la doctrina mayoritaria, del tipo legal vertido en el art. 269A CP no se desprende un claro mandato legal de abandono del sistema informático, sino que, más bien, lo que preexiste es una prohibición de permanecer o de proseguir conectado al sistema informático, cosa que es bien distinta. Prohibición que se suma a la prohibición inicial de acceder al objeto-medio.

Por ello, si bien el deber jurídico preexistente de abandono solo puede ser de naturaleza constitucional o legal, lo cierto es que en la mayoría de los casos tal deber (si fuere un delito de omisión propia) tendría un carácter contractual o convencional con vocación interpartes, por ejemplo, derivado de un contrato de prestación de servicios o un contrato laboral, que obligue

to"; igual en la p. 395; Salvadori (2011a, pp. 776 y 777). En Colombia, con un planteo poco claro y peculiar v. Arboleda Vallejo & Ruiz Salazar (2012, p. 1020), quienes señalan que "Por ello se emplea el verbo "mantener", o sea, permanecer, *no querer salir*" (cursivas propias).

42 Salvadori (2012, p. 380). Lo que implica que no se trataría de una ejecución permanente, sino de una unidad de conducta omisiva.

43 En el mismo sentido se pronuncia el CP, art. 25, inc. 3°, al advertir, frente a los tipos de comisión por omisión, que, "A tal efecto, se requiere que el agente tenga a su cargo la protección en concreto del bien jurídico protegido, o que se le haya encomendado como garante la vigilancia de una determinada fuente de riesgo, conforme a la Constitución o a la Ley".

en concreto al sujeto a abandonar el sistema. El deber de abandono no es lo mismo que la autorización de tratamiento de datos. En este caso, el primer problema típico (dogmático y político-criminal) sería determinar y acordar si esta clase de fuentes interpartes hacen parte de las fuentes legales que exige el CP, art. 10, inc. 2°. El segundo problema, superado el anterior, es que la construcción del "tipo omisivo" a partir de un acuerdo interpartes sería, en principio, contraria al principio de legalidad, no solo porque se dejaría a los particulares la determinación de la estructura del deber que fundamenta el tipo penal, sino también porque la taxatividad del mandato dependería de la redacción de las cláusulas contractuales pertinentes, tal y como lo indica el precepto *contractus ex conventione legem accipere dinoscuntur*[44].

Tercero, debe señalarse que muchos de estos *contratos* solo prevén una autorización para que el sujeto "haga algo concreto" dentro del sistema informático, pero dicha autorización no es equivalente, en términos estructurales, a un mandato jurídico-penal previo de abandonar el sistema, cláusula que debe ser añadida al instrumento contractual. En realidad, si el intérprete deriva un deber de abandono por vía negativa en el caso particular, a partir del principio *contrarius sensus legis pro lege accipitur*[45], se estaría vulnerando la CN (art. 29) y el CP (art. 6°), es decir, transgrediendo la prohibición de la analogía *in malam partem* que, justamente, impide aplicar leyes penales a casos distintos de los comprendidos expresamente por ellas. En conclusión, el intérprete completaría un tipo omisivo inexistente a partir de un deber legal y una norma de mandato hipotética.

Además, tales mandatos no pueden ser cláusulas generales ni mandatos tácitos, porque se desconocería la voluntad real de exclusión del titular del sistema informático. Ello también se desprende del CP, art. 10, porque la regla de taxatividad penal exige la previsión de un deber "claro y delimitado" frente al supuesto típico concreto. Una modalidad de deberes generales son los contenidos en la L. 1581 de 2012/ arts. 17 "Deberes de los responsables del tratamiento" y 18 "deberes de los encargados del tratamiento"[46], que difícilmente podrían fundamentar un tipo de omisión propia por sí mismos.

Finalmente, *cuarto*, recuérdese que el acceso abusivo al sistema informático no siempre es realizado por un sujeto activo que tenga la calidad de *insider*, es decir, que tenga cierta auto-

44 Domingo & Rodríguez-Antolín (2000, p. 38, No. 108), señalan: "(Bonifacio VIII, *Liber sextus* 5.12.85) Los contratos se distinguen por recibir la ley de la propia convención (…)".

45 Domingo & Rodríguez-Antolín (2000, p. 38, No. 110), advierten: "(Azón, *Brocarda,* rúbrica 18 folio 56). El sentido contrario de la ley es tenido por ley. La interpretación *a sensu contrario* es una exigencia de cualquier interpretación atenta al espíritu y finalidad de la norma (…)".

46 L. 1581 de 2012/art. 17: "Los Responsables del Tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad: c) Informar debidamente al Titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada; d) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento; i) Exigir al Encargado del Tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del Titular " y art. 18: "Los Encargados del Tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad: b) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento; j) Permitir el acceso a la información únicamente a las personas que pueden tener acceso a ella". Verdaderos deberes abstractos que no fundamentan el mandato concreto de ningún tipo omisivo en la legislación nacional.

rización previa y limitada para acceder al sistema, que luego es desconocida, ya que el delito también puede ser realizado por un sujeto *outsider* que no tenga ninguna clase de autorización o cuando haya ingresado al sistema de manera accidental o casual.

En todo caso, el asunto no es de simple forma porque está íntimamente relacionado con la naturaleza de la norma primaria que protege el tipo penal analizado.

b) Una segunda postura, mayoritaria en la doctrina, sostiene que el 'mantenerse' o proseguir en el sistema informático es una conducta comisiva dolosa, cuyo fundamento de acriminación radica en el hecho de mantener abusivamente un diálogo lógico con el sistema en contra de la voluntad de quien tenga el derecho legítimo de excluir a terceros[47]. Desde esta perspectiva, que consideramos correcta, la base normativa del tipo consiste en infringir discontinuamente una prohibición de *permanencia*, una vez haya terminado la autorización previa del titular para permanecer en el medio-objeto, o cuando el titular le haya expresado al sujeto activo, por cualquier medio, su condición de extraño o intruso en aquellos casos en los que el ingreso inicial fue accidental o fortuito.

Naturalmente, de la prohibición típica de proseguir el nexo lógico se advierte, *contrario sensu* (como la otra cara de la moneda), el deber de *hacer log-out* (acción de referencia negativa); pero lo cierto es que ello no hace del tipo una figura de naturaleza omisiva[48]. En fin, consideramos que si fuese una "omisión pura" el legislador penal colombiano la hubiera construido (determinado) mediante expresiones como, por ejemplo, "o no salga del sistema en contra de la voluntad [...]", "o no se desconecte del sistema en contra de la voluntad [...]", significando así el mandato de terminar el nexo lógico.

Es más, considérense aquellas hipótesis en las que el sujeto activo del tipo tiene que ejecutar "manipulaciones informáticas"[49] para sortear o superar las contramedidas de seguridad dispuestas por el *owner,* con el propósito de excluir al intruso del sistema informático, o cuando este deba interactuar con el software para ocultarse y lograr permanecer dentro de todo o una parte del mismo.

Por ello, se afirma que el injusto de la prohibición radica en lesionar de manera permanente la integridad de los sistemas informáticos, y poner en peligro concreto —en los términos vistos—

47 V. Posada Maya (2006b, p. 27); Pabón Parra (2011, pp. 499-500), al afirmar que "La acción de "mantenerse" implica el ingreso legítimo del agente al respectivo medio informático y la prolongación ilegítima de su permanencia en el mismo, contrariando la voluntad de quien tiene el derecho de exclusión". En la doctrina extranjera v. Anarte Borallo (2003, p. 238); Mantovani (2008, pp. 520 y 522), quien define el mantenerse como persistir en la ya iniciada introducción, inicialmente autorizada o casual, el continuar y acceder al conocimiento de los datos.

48 Velásquez Velásquez (2009, pp. 659 y ss.), señala que: "(…) mientras en las conductas de comisión dolosa la tipicidad emana de la identidad entre la conducta causal-final-social llevada a cabo con la descrita en la ley, en las omisivas ella surge de la diferencia entre el actuar realizado y el vertido en el dispositivo legal respectivo; ese contraste se deriva del hecho de que la norma antepuesta al tipo activo es *prohibitiva*, mientras que detrás del omisivo subyace una de carácter imperativo".

49 Posada Maya (2013, p. 13), define las manipulaciones informáticas en sentido amplio como "[...] una acción preparatoria ilegítima dirigida a introducir o almacenar datos incorrectos e incompletos, o a adulterar los almacenados en un sistema informático o telemático; y ii) a la manipulación o pre-ordenación de los resultados de un proceso de elaboración o transmisión de datos almacenados, mediante la configuración, alteración o modificación de las instrucciones originales de los programas que tratan los datos o la información de entrada (*input*) o salida (*output*) auténtica de los programas o *software* […]". También en Posada Maya (2006b, p. 46).

la intimidad informática de los datos o informaciones almacenados en ellos, mientras dure la conexión o el mantenimiento no autorizados.

En tercer lugar, el tipo penal es de medios abiertos. Esto significa —consideradas las precisiones hechas al analizar la acción 'mantenerse'— que los verbos rectores se pueden realizar de cualquier forma, siempre que esta sea informática. Por ejemplo, se ha dicho que el acceso puede ser directo o remoto en términos técnicos. Asimismo, el tipo penal puede conllevar, como medio necesario e inherente para ejecutar el acceso, que el sujeto activo utilice datos falsos o datos correctos pero de manera ilegítima, cuestión que podría plantear un aparente concurso de tipos con el delito de violación de datos personales CP/art. 269F).

Finalmente, el art. 269H, nums. 3 y 7 permite modificar esta figura cuando: a) el sujeto aproveche la confianza depositada por el dueño del sistema informático, lo que supone un mayor desvalor de acción objetivo por la forma de comisión del comportamiento —cuando el novio accede abusivamente a la cuenta de correo de su novia, el cónyuge varón al Messenger de la cónyuge, etc.—. Y b) cuando el sujeto realice el acceso o el mantenimiento utilizando como instrumento a un tercero de buena fe. Esta agravante supone, en principio, un mayor desvalor de acción objetivo por la forma en que se facilita la comisión del delito. No obstante, recuérdese que la autoría mediata[50] supone realizar el tipo penal *utilizando a otro como instrumento*, lo que permite aplicar el tipo fundamental a dicho título. Por ello parece contrario al *ne bis in idem* castigar el delito de acceso a título de autoría mediata y luego agravar el comportamiento porque el autor mediato ha utilizado a un instrumento o a un tercero de buena fe en la ejecución delictiva (que actúa sin dolo).

En cuarto lugar, si bien las modalidades típicas pueden ser realizadas en cualquier clase de terminal pública o privada —conectada o no a la Internet o a una intranet—, se debe aclarar que el comportamiento sería atípico (absoluto) cuando el sistema informático no sea de acceso restringido. De este modo, no habría delito si el sujeto accede a un sistema en el que solo se han dispuesto advertencias referidas a la prohibición genérica de acceder sin la observancia de ciertas condiciones como, por ejemplo, cumplir con cierta edad o estar en un determinado lugar o país.

También será atípico el comportamiento del CP art. 269A, como se dijo, cuando se acceda a un sistema informático público o de libre acceso para terceros, cuando se obtengan medios de almacenamiento o cuando el sujeto conozca información de terceros sin haber accedido previamente al sistema de manera ilegal.

En quinto lugar, en Colombia, en razón del principio de legalidad de los delitos, no es punible la omisión de protección de datos o información informatizada sensible o reservada que un sujeto haya almacenado en un sistema informático desprotegido. No hay tipo penal concreto. Ello, no obstante que la sola tenencia de los datos o información sensible constituya una *actividad peligrosa* para la intimidad personal, precisa-

50 CP, art. 29, inc. 1°: "Es autor quien realice la conducta punible por sí mismo *o utilizando a otro como instrumento*" cursivas por fuera del texto original.

mente, porque esta se encuentra por fuera de la posibilidad de custodia por parte de sus legítimos titulares. Sobre este asunto se ha dicho con anterioridad que:

> [...] desde una perspectiva político-criminal no parece adecuado librar de responsabilidad al titular del sistema informático, en aquellos casos en que, o bien de manera insegura o con simples advertencias expone al público contenidos legalmente regulados que requieren controles de acceso y de seguridad para cierta población protegida (pornografía), o cuando los datos o información de terceros sean manipulados o conocidos por intrusos debido a la omisión de controles previos en el ámbito de dominio específico de los titulares de sistemas informáticos. (Posada Maya, 2006b, pp. 26-27)[51].

Finalmente, en *sexto lugar*, el acceso *no puede ser consentido* o autorizado, y si lo es, la acción del sujeto activo, para ser punible, debe exceder lo acordado por las partes de manera expresa y clara[52]. Salvo en los casos de acceso accidental o casual, dicho consentimiento no solo se debe entender como la oposición al acceso o al mantenimiento por aquel sujeto que tenga la capacidad legítima de disponer del sistema informático, sino como la ausencia de facultades jurídicas *ex ante* para realizar un acceso o para mantenerse dentro de este.

Naturalmente, si el sujeto activo consiente *ex ante* la realización del acceso o de la permanencia, la conducta será plenamente atípica, según lo prevé el CP, art. 32, num. 2, a pesar de tratarse de un delito que afecta intereses colectivos.

En este sentido, la L. E. 1581 de 2012/art. 6° especifica que "Se prohíbe el Tratamiento de datos sensibles, excepto cuando: a) El Titular haya dado su autorización explícita a dicho Tratamiento, salvo en los casos que por ley no sea requerido el otorgamiento de dicha autorización", entre otros supuestos legales[53]. Autorización que el responsable del tratamiento tiene el deber legal de conservar en copia, según lo indica el art. 17 *ibidem*.

Para terminar este acápite, debe tenerse en cuenta que, en los casos de autorización *ex ante*, la facultad jurídica para acceder o para mantenerse en el sistema puede ser total o parcial. De ahí la importancia de que la autorización siempre sea clara para evitar dudas acerca de lo que el sujeto activo puede o no hacer. Puede acontecer que el titular del sistema informático

51 También: Posada Maya (2006a, p. 63), aunque el artículo está referido al derogado art. 195 del CP, que exigía de manera expresa que el sistema informático estuviera protegido con medida de seguridad informática. En todo caso, la conclusión de dicho comentario sigue vigente: "Se ha hecho evidente que la protección jurídico penal en materia de intrusión informática no es integral, de cara a la protección del derecho fundamental a la intimidad, cuando terceros poseen o administran información de naturaleza sensible, almacenada en sistemas informáticos que carecen de medidas de salvaguarda, precisamente por omisión dolosa de los titulares o administradores del sistema informático intrusado".

52 En otros ordenamientos penales como el italiano (CP, art. 615ter), la voluntad de exclusión puede ser expresa o *tácita*. V. Salvadori (2012, pp. 370-381).

53 Art. 6°: los demás supuestos son: "b) El Tratamiento sea necesario para salvaguardar el interés vital del Titular y este se encuentre física o jurídicamente incapacitado. En estos eventos, los representantes legales deberán otorgar su autorización; / c) El Tratamiento sea efectuado en el curso de las actividades legítimas y con las debidas garantías por parte de una fundación, ONG, asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refieran exclusivamente a sus miembros o a las personas que mantengan contactos regulares por razón de su finalidad. En estos eventos, los datos no se podrán suministrar a terceros sin la autorización del Titular; / d) El Tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial; / e) El Tratamiento tenga una finalidad histórica, estadística o científica. En este evento deberán adoptarse las medidas conducentes a la supresión de identidad de los Titulares".

solo haya consentido un acceso temporal a todo o a parte del sistema informático, o que la autorización tenga un límite definido en el tiempo. En estos casos se tendrá que verificar si el sujeto activo abusó del tiempo concedido (abuso *extra tempore*) o si accedió o se mantuvo en una parte vedada del sistema (abuso *extra loco*), por fuera de lo acordado con el titular. También puede suceder que el sujeto pasivo haya autorizado el ingreso del sujeto activo a todo o a parte del sistema informático, con limitación o no de partes, pero con el fin de desarrollar tareas concretas de actualización, limpieza o instalación de datos, corrección o actualización de cierto software, etcétera. En estos casos, además, habría que verificar qué clase de actuaciones lógicas fueron ejecutadas dentro del sistema[54].

7. No se requiere un *nexo de causalidad*

Como quiera que el tipo penal estudiado sea de mera conducta, no se requiere entonces verificar la existencia de un nexo de causalidad. Sin embargo, en estos casos virtuales es necesario reemplazar este elemento por un *nexo de naturaleza lógica* que implique determinar la existencia de un diálogo informático entre el autor y el sistema informático, que obedezca a la interacción *input-output* propiciada por las instrucciones electrónicas imputadas al sistema por el sujeto activo y respondidas por la máquina conforme al tratamiento de los datos o al software correspondiente, según el propósito del autor.

Además, la lesión a la integridad informática y el peligro para la intimidad o reserva de datos e información personal almacenada en el sistema tienen que poder serle imputados objetivamente al sujeto activo (o coautores). Así, en primer lugar, el acceso o el mantenimiento debe involucrar un riesgo jurídicamente desaprobado para el bien jurídico, y en particular para las funciones informáticas propiamente dichas (disponibilidad, integridad y seguridad de los sistemas informáticos). Asimismo, es fundamental acreditar que el intruso haya tenido el dominio del hecho sobre la introducción de las órdenes dadas al sistema operativo informático. El comportamiento se agrava según el CP, art. 269H, num. 6, cuando el riesgo comprometa la seguridad o la defensa nacional de Colombia, lo que implica un mayor desvalor de resultado.

En segundo lugar, el riesgo informático creado debe traducirse en el resultado jurídico típico informático, esto es, la lesión a la integridad, disponibilidad y confiabilidad del sistema informático, como ya se indicó.

Y finalmente, en tercer lugar, la afectación al bien jurídico debe quedar cubierta por los riesgos prohibidos incluidos en el diseño de la norma prohibitiva. En caso de no existir alguna posibilidad de afectación (directa o indirecta) a los bienes jurídicos protegidos por la acción informática abusiva, en particular a la integridad del sistema informático y a la intimidad informática, no cabría hablar de esta figura criminal (Silva Sánchez & otros, 2011)[55]. Ejemplo de ello sería cuando se accede a un PC nuevo u otro que

54 En sentido similar: Salvadori (2012, p. 374).

55 Aunque referido al derecho español, estos autores entienden que la protección del honor y la intimidad personal y familiar comportaría "[…] una exigencia adicional: que el sistema informático contenga datos relativos a la vida privada o íntima de las personas, aunque no es necesario que se llegue a acceder a ellos".

no tenga datos personales, salvo que el autor tenga la intención de instalar un troyano u otro programa malicioso o dañino. Por fuera de este caso, el acceso al sistema sería insignificante si el agente no tiene la posibilidad de disponer, al menos un instante, de los datos personales o la información informatizada almacenada en ellos.

En fin, en las hipótesis de acceso abusivo a sistema informático se discute ampliamente si los actos de autopuesta en peligro realizados por el sujeto pasivo tienen incidencia específica en la imputación de los posibles peligros que ejecute el sujeto activo frente a la seguridad de la información, los datos y el sistema informático en particular. ¿Cómo el riesgo de acceso o mantenimiento se materializa en una afectación a la integridad del sistema informático, cuando el sujeto pasivo tenga un sistema informático que *per se* está en peligro porque no está protegido por negligencia o voluntad del titular, o debido a que las medidas de seguridad informáticas instaladas resultan irrisorias, inidóneas o inadecuadas para protegerlo, según los parámetros de gestión informática vigentes? La respuesta no es clara, entre otras cosas porque el solo acceso afecta a la integridad del sistema informático al modificar sus archivos operativos, y porque el legislador ha eliminado toda exigencia de autorresponsabilidad por parte del titular (del sistema y los datos), cuando no exige que el medio esté protegido previamente con una medida de seguridad informática.

Es irrelevante, entonces, si el titular no ha tomado medidas de protección, es decir, si ha provocado un *suicidio informático*, incluso de manera imprudente.

B. Aspecto subjetivo

1. Dolo (CP, art. 22)

Se requiere que el sujeto activo conozca y quiera la realización de una conducta dirigida: en primer lugar, a acceder a todo o a una parte de un sistema informático, esto es, a un sistema de tratamiento, procesamiento y transmisión automática de datos informatizados y, en segundo lugar, a mantenerse o permanecer dentro del sistema en contra de la voluntad del legítimo titular. En principio, la conducta requiere dolo directo, pues su comisión a título de dolo eventual es extremadamente improbable.

El conocimiento del dolo deberá abarcar en concreto: a) las circunstancias de hecho que establecían la existencia de facultades positivas o la autorización del sujeto activo (no su contenido), o el ámbito fáctico de la autorización *ex ante* para acceder o para mantenerse dentro del sistema informático (o usar ciertos programas), es decir, debe haber un dolo de abuso; b) la creación o mantenimiento de un diálogo o nexo lógico con el sistema informático y, de modo general, c) el plan de ataque informático que pueda incluir las posibles manipulaciones informáticas requeridas para desarrollar la conducta prevista en el CP, art. 269A. El dolo se prueba a través de los medios de prueba dispuestos en la legislación procesal vigente (CPP, L. 906 de 1994/ arts. 372 y ss.). A diferencia del CP, art. 195 original, ya no es necesario conocer que el sistema haya estado protegido con una medida de seguridad para derivar el dolo típico.

2. Ánimo especial

A diferencia de las normativas y convenios internacionales citados, infortunadamente el tipo penal de acceso abusivo a sistema informático previsto en el CP, art. 269A, no exige al sujeto activo actuar con un ánimo especial o un elemento subjetivo especial distinto del dolo, que requiera la intención de acceder al sistema informático para realizar conductas ilícitas posteriores como, por ejemplo, el ánimo de lucro, la *violación o interceptación de datos personales* (CP, arts. 269 C y F), el *sabotaje o daños informáticos* (CP, art. 269 D) u *obstaculización ilegítima del sistema informático* (CP, art. 269B) o el uso del sistema en contra de los reglamentos, entre otras conductas[56].

Ello implica que el tipo penal solo exige un dolo avalorado, en cuya virtud se castigan comportamientos que no suponen una verdadera finalidad criminal ulterior, como sucede con el *hacking* blanco o *joyriding* que, según la doctrina, se presenta cuando jóvenes perpetran actos de acceso no autorizados a sistemas informáticos con el propósito de demostrar la vulnerabilidad del sistema, por motivos de curiosidad o desafío intelectual[57]. No importa que el sujeto activo pueda conocer datos operativos del sistema. Otro ejemplo sería el acceder al sistema para enviar un correo electrónico, para leer la prensa digital o para hacer una carta urgente, entre otras actuaciones irrelevantes.

En efecto, la precisión del elemento subjetivo constituye una buena práctica político-criminal para reducir el ámbito de aplicación del tipo penal de amenaza, cuando se corra el peligro de cubrir comportamientos inofensivos que, en verdad, solo impliquen riesgos objetivamente desvalorados, riesgos accidentalmente peligrosos o riesgos francamente irrelevantes o insignificantes. Por ejemplo, en el caso del acceso informático, para algún sector de la doctrina el peligro contra la reserva o intimidad de los datos no parece satisfecho con el simple acceso o ingreso del "intruso", sin que tal conducta se acompañe de una finalidad que demuestre el deseo de ejecutar conductas posteriores dentro del sistema, contra este o sobre los datos o la información sensible del titular del bien jurídico allí almacenada (como lo demuestra la mayoría de los tipos penales de *lege ferenda*).

Finalmente, hay que recordar que el CP, art. 269H, num. 6, permite agravar y modificar el tipo penal cuando el sujeto realice la conducta de acceso o mantenimiento con fines terroristas, esto es, en los términos del CP, art. 343, con el fin de causar zozobra o terror en la población civil o a algún sector de ella. Sin que tal efecto psicológico se tenga que hacer efectivo, pues basta el simple fin —como mayor desvalor de acción subjetivo— para que se pueda agravar la figura. Tampoco se requiere que el sujeto activo tenga que sustraer datos, dañar informa-

56 Morillas Cueva (2011, p. 321), Quintero Olivares & Morales Prats (2011a, p. 484), Rueda Martín (2009, p. 160).

57 Sobre el particular, v. González Rus (2006, pp. 241-247). Se podría eliminar la medida de seguridad a condición de que se exija la finalidad: Morón Lerma (2002, pp. 39 y ss.). A favor del castigo, v. también Rovira del Canto (2002, pp. 196 y ss.), quien indica que dicha conducta entraña la producción de un perjuicio de peligro de los intereses económico-patrimoniales contenidos en los programas o en los datos a los que tiene acceso o la pérdida de esfuerzo o costo que le ha supuesto al titular establecer medidas de seguridad. A su turno, Rueda Martín (2009, p. 188) señala que "Lo que no puede aceptarse es que se haya descubierto la vulnerabilidad de un sistema y producido el acceso, no se informe de ningún modo a los administradores o a los encargados de la seguridad de los sistemas".

ción u obstaculizar el sistema informático, entre otras conductas delictivas alternas.

C. Concurso de delitos

Más complejo es el tema del concurso (aparente o efectivo[58]) de tipicidades tratándose de los delitos informáticos, precisamente, porque el legislador ha diseñado el castigo de estas figuras criminales sin considerar que constituyen actos previos o posteriores del *iter criminis* de otros tipos penales, con lo cual el solapamiento de unos y otros, o la consunción por hecho acompañante de unos por otros, es un fenómeno jurídico normal. Situaciones que también tienen explicación por el castigo excesivo de actos preparatorios o por el adelantamiento —extravagante— de las barreras de protección de la seguridad de la información, los datos y los sistemas informáticos.

Así las cosas, antes de ser ejecutado un acceso abusivo a un sistema informático es común advertir, por ejemplo, cómo los criminales crean y suplantan sitios web para capturar datos personales como *paswords* o claves (CP, art. 269G, subsidiario cuando no exista un delito sancionado con pena más grave), usan software malicioso (CP, art. 269E) o violan datos personales contenidos en ficheros, bases de datos o medios semejantes, mediante conductas de obtención, sustracción, intercambio, compra o interceptación de datos (CP, art. 269 F y C), que luego se emplean para acceder al sistema informático atacado (CP, art. 269A).

Asimismo, luego del acceso o del mantenimiento doloso, también se pueden llevar a cabo otras actividades ilícitas como, por ejemplo, violaciones o interceptaciones de datos (CP, art. 269 F y C), conductas de obstaculización ilegítima del sistema (CP, art. 269B), daños informáticos (CP, art. 269D), transferencia no consentida de activos y hurtos por medios informáticos, entre otros. Así, en el caso de que la violación de datos sea previa al acceso o al mantenimiento abusivo se podría configurar un concurso efectivo de tipicidades. Por el contrario, si el acceso es previo a la violación y no se ponen en peligro bienes jurídicos diferentes a los de los sujetos pasivos, en principio, la violación de datos subsumiría materialmente (delito medio a delito fin) el acceso abusivo, aunque no faltarán autores que crean que el acceso o el mantenimiento consumado constituyen una tentativa de violación de datos personales, cuando no se logre consumar alguno de los verbos rectores previstos en la norma que requieran un resultado material (Rueda Martín, 2009, p. 169).

Es más, muchas de estas figuras criminales requieren, necesariamente, que el sujeto activo del tipo penal acceda al sistema informático mediante manipulaciones informáticas para superar los mecanismos de validación o identificación (*login* y *pasword*), como ocurre, por ejemplo, con el delito de transferencia no consentida de activos (Posada Maya, 2013), que vendría a subsumir materialmente (como delito fin) la violación de datos personales (como delito medio), aunque no cobijaría el delito de acceso abusivo al sistema, porque tal hipótesis dejaría de castigar el peligro creado para la intimidad informática y la lesión para la integridad del sistema

58 Sobre este tema v. Posada Maya (2012 pp. 172 y ss.).

informático, como objeto-medio sobre el cual recae la acción criminal. El tema es muy complejo, pero debe ser analizado caso a caso.

III. CONCLUSIONES

El delito de acceso abusivo a sistema informático previsto en el CP, art. 269A, no es un delito común sino un cibercrimen caracterizado por exigir especiales formas y métodos de ejecución propiamente informáticos, contra objetos-medio inmateriales (sistemas informáticos), realizado por sujetos que usualmente tienen perfiles criminológicos muy precisos. Su interpretación siempre gravita en torno de un bien jurídico autónomo (colectivo-individual) definido como la seguridad, integridad y disponibilidad de la información, los datos y los sistemas informáticos. Actuación que puede vulnerar otros bienes jurídicos, como sucede con la intimidad personal informática (Boix Reig & otros, 2010, p. 457).

El legislador penal colombiano ha empleado una técnica legislativa muy discutible al consagrar los delitos de intrusión informática, al menos por tres razones. En primer lugar, porque la norma se aparta de dos aspectos sugeridos por la doctrina en esta materia, lo que refuerza la desventajosa naturaleza de la descripción típica como un delito de mera conducta, lesión contra el sistema informático y peligro potencial para los datos y la autodeterminación informática.

En segundo lugar, la eliminación de las medidas de seguridad informáticas dispuestas para limitar el acceso de terceros al sistema informático. Aspecto que resquebraja el principio de autorresponsabilidad del titular del sistema y condiciona la aplicación de figuras como la autopuesta en peligro, cuando se trata de estudiar la imputación objetiva, tal y como ha quedado dicho a lo largo del texto.

Desde un punto de vista subjetivo, el tipo penal parece configurar una cláusula general, toda vez que no exige la ejecución del acceso o del mantenimiento abusivo con una finalidad ilícita ulterior, como lo sería, por ejemplo, el ánimo de lucro, el propósito de violar, interceptar, borrar, copiar o sustraer datos personales del sujeto pasivo o de terceros que se encuentren almacenados en el sistema informático. De algún modo, la precisión de dichos elementos subjetivos permitiría acotar la clase de peligro típico requerido contra el bien jurídico en su aspecto individual, es decir, la intimidad y autodeterminación informáticas.

Del mismo modo, el poder sancionar actuaciones sin alguna finalidad específica permite tipificar los casos, en principio inofensivos, de *hacking blanco* realizados por adolescentes o por personas que solo buscan, por motivos intelectuales o por el simple reto, desafiar las seguridades de un sistema informático determinado. Lo que comporta una extravagante anticipación de la barrera de protección del bien jurídico protegido.

En tercer lugar, el tipo penal fue diseñado como una conducta de lesión frente a la integridad del sistema informático y de peligro en abstracto para la intimidad informática. Peligro que se puede interpretar, en los términos del art. 11

del CP, como un peligro concreto contra la reserva o intimidad informática del sujeto pasivo, cuando la intrusión suponga la posibilidad fáctica —al menos un instante— de obtener servicios, causar daño o disponer de la información sensible existente y retirarla de aquel. De todas maneras, este tipo de regulaciones quiebra el andamiaje demoliberal dispuesto por el CP y por los sistemas de juzgamiento en nuestro medio, que se basan en la posibilidad de discutir la imputación, su ofensividad y la culpabilidad por la realización del hecho.

Bibliografía

Álvarez García, F. J., & otros. (2011). *Derecho penal español. Parte especial.* Valencia: Tirant lo Blanch.

Álvarez García, F., & otros. (2011). *Derecho penal español, parte especial.* Valencia: Tirant lo Blanch.

Anarte Borallo, E. (2003). Sobre los límites de la protección penal de datos personales. *Derecho y Conocimiento,* 225-254.

Arboleda Vallejo, M., & Ruiz Salazar, J. A. (2012). *Manual de derecho penal, partes general y especial* (11 ed.). Bogotá: Leyer.

Boix Reig, J., & otros. (2010). *Derecho penal español. Parte especial.* Vol. I. Madrid: Iustel.

Cano M., J. J. (2009). *Computación forense: descubriendo los rastros informáticos.* México: Alfaomega.

Cano Martínez, J. J. (coord). (2010). *El peritaje informático y la evidencia digital en Colombia. Conceptos, retos y propuestas.* Bogotá: Uniandes-GECTI.

Castro Ospina, S. J. (2001). Delitos informáticos: la información como bien jurídico y los delitos informáticos en el nuevo Código Penal Colombiano. En *XXIII Jornadas internacionales de derecho penal, Memorias* (págs. 127-162). Bogotá: Universidad Externado de Colombia.

De la Cuesta Arzamendi, J. L., & otros. (2010). *Derecho penal informático.* Navarra: UPV-Civitas-Thomson Reuters.

De la Mata Barranco, N., & Díaz Hernández, L. (2010). Delitos vinculados a la informática en el dereho penal español. En *Derecho penal informático.* Madrid: Universidad del País Vasco e Instituto Vasco de Criminología, Civitas-Thomson-Reuters.

Del Pino, L. (2009). *Diritto Penale, Parte speciale* (17 ed.). Napoli: Eizioni Giuridiche Simone.

Domingo, R., & Rodríguez-Antolín, B. (2000). *Reglas jurídicas y aforismos.* Navarra: Aranzadi.

Fernández Teruelo, J. G. (2011). *Derecho penal e Internet: especial consideración de los delitos que afectan ajóvenes y adolescentes.* Valladolid: Lexnova.

Fiandaca, G., & Musco, E. (2007). *Diritto penale, Parte speciale* (3 ed.), vol. I. Padova: CEDAM.

García González, J. (2006). Intervenciones de terceros en el correo electrónico. Especial re-

ferencia al ámbito laboral y policial. En C. M. Casabona, & otros, *El ciber criminen, nuevos retos jurídico-penales, nuevas respuestas político-criminales.* Granada: Comares.

González Rus, J. J. (2006). Los ilícitos en la red (i): hackers, crackers, ciberpunks, snifers, denegación de servicio y otros comportamientos semejantes. En C. M. (Coord.), *El cibercrimen, nuevos retos jurídico-penales, nuevas respuestas político-criminales.* Granada: Comares.

Kindhäuser, U. (2009). *Strafrecht, Besonderer Teil* (4 auf. ed.), vol. I. Baden-Baden: Nomos.

Krey, V., Heinrich, M., & Hellmann, U. (2012). *Strafrecht, Besonderer Teil* (15 auf. ed.). Stuttgart: W. Kohlhammer.

Mantovani, F. (2008). *Diritto Penale, parte speciale. Delitti contro la persona* (3 ed.), vol. I). Padova: CEDAM.

Matellanes Rodríguez, N. (2000). Algunas notas sobre las formas de delincuencia informática en el Código Penal. En M. D. Diego Díaz-Santos, & V. Sánchez López, *Hacia un derecho penal sin fronteras,* (pp. 129-147). Madrid: Colex.

Morillas Cueva, L. (2011). *Sistema de derecho penal español, Parte especial.* Madrid: Dykinson.

Morón Lerma, E. (2002). *Internet y derecho penal: hacking y otras conductas ilícitas en la Red.* Navarra: Aranzadi.

Nomos Gesetze, S. (2011). *Nomos Gesetze, Strafrecht* (20 auf. ed.). Baden-Baden: Nomos.

Pabón Parra, P. A. (2011). *Manual de derecho penal, Parte especial* (8 ed.), vol. 2. Bogotá: Doctrina y Ley.

Palazzi, P. A. (2009). *Los delitos informáticos en el Código Penal.* Buenos Aires-Bogotá-México: Abeledo Perrot.

Picotti, L. (2006). Internet y derecho penal: ¿un empujón únicamente tecnológico a la armonización internacional?. En *El cibercrimen, nuevos retos jurídico-penales, nuevas respuestas político-criminales.* Granada: Comares.

Picotti, L. (2006). Los datos de carácter personal como bienes jurídicos penalmente protegidos. En AA. VV., *El cibercrimen, nuevos retos jurídico-penales, nuevas respuestas político-criminales.* Granada: Comares.

Polaino Navarrete, M. (2011). *Lecciones de derecho penal, parte especial,* vol. I. Madrid: Tecnos.

Polaino Navarrete, M., & otros. (2010). *Lecciones de derecho penal, parte especial,* vol. 1. Madrid: Tecnos.

Polaino Navarrete, M., & otros. (2011). *Lecciones de derecho penal. Parte especial,* vol. 2. Madrid: Tecnos.

Posada Maya, R. (2006a). ¿Es integral la protección jurídico penal por intrusión informá-

tica para titulares de información reservada? *Revista Sistemas (Seguridad y Computación forense)* (96), págs 56-63.

Posada Maya, R. (2006b). Aproximación a la criminalidad informática en Colombia. *Revista de derecho, comunicaciones y nuevas tecnologías* (2), págs 11-60.

Posada Maya, R. (2012). *Delito continuado y concurso de delitos.* Bogotá: Uniandes-Ibáñez.

Posada Maya, R. (2013). El delito de transferencia no consentida de activos. *Revista de Derecho, Comunicaciones y Nuevas Tecnologías* (8).

Queralt Jiménez, J. J. (2010). *Derecho penal español, parte especial* (6 ed.). Barcelona: Atelier.

Quintero Olivares, G., & Morales Prats, F. (2011). *Comentarios a la parte especial de derecho penal* (9 ed.). Navarra: Aranzadi Thomson Reuters.

Quintero Olivares, G., Morales Prats, F., & Otros. (2011). *Comentarios al Código Penal español, artículos 1 a 233* (6 ed.), vol. I). Navarra: Aranzadi Thomson Reuters.

Rengier, R. (2011). *Strafrecht, Besonderer Teil* (12 ed.), vol. 2). München: verlag C. H. Beck.

Rey Boek, A., & Nuñez de León, C. (2011). De los delitos informáticos. Ley 1276 de 2009. En Ob. Col. al, *Manual de derecho penal, parte especial,* (Vol. II, pp. 624-633). Bogotá: Temis-U. Rosario.

Rodríguez Moro, L. (2011). Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio. En J. M. Terradillos Basoco, & otros, *Lecciones materiales para el estudio del derecho penal (T. 3), Derecho Penal, Parte Especial, v*ol. I. Madrid: Iustel.

Romeo Casabona, C. M. (2006). De los delitos informáticos al cibercrimen. Una aproximación conceptual y político-criminal. En C. M. al, *El cibercrimen, nuevos retos jurídico-penales, nuevas respuestas político-criminales* (pp. 1-42). Granada: Comares.

Rovira del Canto, E. (2002). *Delincuencia informática y fraudes informáticos.* Granada: Comares.

Rueda Martín, M. Á. (2009). Los ataques contra los sistemas informáticos: conductas de Hacking. Cuestiones poítico-criminales. *Revista Jurídica on line, 7* (26), págs 157 y ss.

Salvadori, I. (2011). I nuovi reati informatici introdotti nel codice penale spagnolo con la legge organica N.5/2010. Profili di diritto comparato. *L'indice penale, Nuova Serie- Anno XIV* (2), págs 767 y ss.

Salvadori, I. (2011). Los nuevos delitos informáticos introducidos en el Código Penal español con la ley Orgánica 5/2010. Perspectiva de derecho comparado. *ADPCP, LXIV*, págs 221 y ss.

Salvadori, I. (2012). Quando un insider accede abusivamente ad un sistema informatico o telematico? Le sezionni unite precisano l'ambito di aplicazione dell'art. 615ter CP. Comenti a Sentenza Cass., s.u. 27.10.2011 (dep. 7.2.2012), n. 4694. *Rivista trimestral di diritto penale dell'economia* (1-2), págs 369 y ss.

Schmidt, R., & Priebe, K. (2010). *Strafrecht - Besonderer Teil.* (8 auf. ed., Vol. II). Bremen: Grasberg.

Silva Sánchez, J. M., & otros. (2011). *Leciones de derecho penal, parte especial* (3 ed.). Barcelona: Atelier-Iuscrimbcn.

Velasco San Martín, C. (2012). *La jurisdicción y competencia sobre delitos cometidos a través de sistemas de cómputo e Internet.* Valencia: Tirant lo Blanch.

Velásquez Velásquez, F. (2009). *Derecho penal, Parte general 4ª ed.* Medellín: Comlibros.

Wessels, J., & Hettinger, M. (2011). *Strafrecht BesondererTeil, Straftaten gegen Persönlichkeits und Gemeinschaftswerte* (35 auf. ed., Vol. 1). Heidelberg: C.F. Müller.